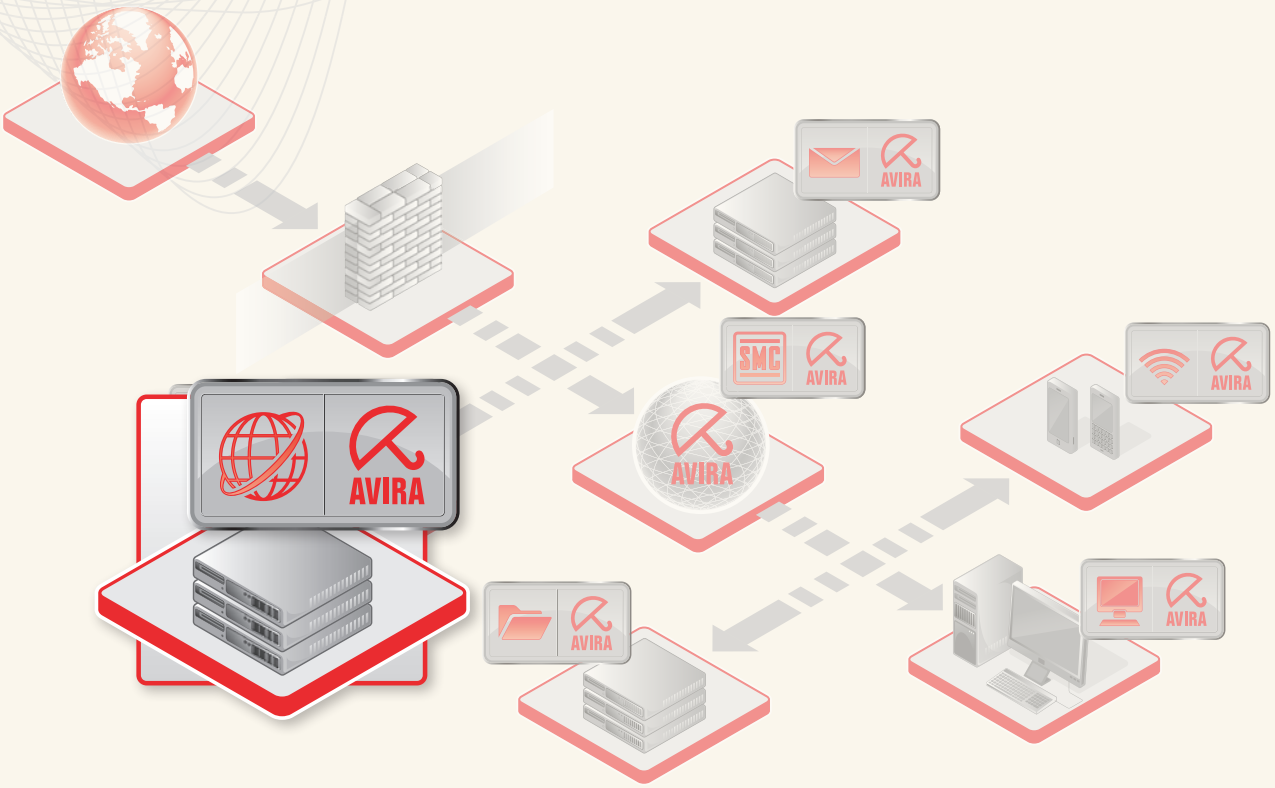
AVIRA
More Than Security

User Manual

Avira AntiVir Exchange 7

Avira AntiVir Exchange 2000/2003
Avira AntiVir Exchange 2007



www.avira.com

Contents

1 Getting Started 6
1.1 Installation on an Exchange Server 6
1.2 Starting AntiVir Exchange Management Console 6
1.3 Configuration in AntiVir Exchange Management Console 6
1.3.1 Required Basic Configuration Steps 7
1.3.2 Required Policy Configuration Steps 7
1.3.3 Recommended Basic Configuration Steps 8
1.3.4 Virus Scanning in Exchange Databases 8
1.4 Observing Data in AntiVir Monitor 8
2 Installation 9
2.1 System Requirements 9
2.2 Installation of the Virus Scanner 9
2.3 Installation of Avira AntiVir Exchange on an Exchange Server 9
2.4 Uninstallation of Avira AntiVir Exchange 7 13
3 General 15
3.1 The Architecture of Avira AntiVir Exchange 15
3.1.1 AntiVir Exchange Management Console 15
3.1.2 Avira AntiVir Exchange Server 16
3.1.2.1 Grabber 16
3.1.2.2 Avira AntiVir Exchange Service = Enterprise Message Handler (EMH) 16
3.1.2.3 Avira AntiVir Exchange Quarantine 17
3.1.2.4 Active Directory / LDIF 18
3.1.2.5 Compressed Files and Archives: Avira AntiVir Exchange Unpacker 18
3.1.3 Avira AntiVir Exchange Configuration 18
3.2 User Interface 19
3.2.1 Toolbar 20
3.2.2 Icons 21
3.3 Configuration in AntiVir Exchange Management Console 22
3.3.1 Basic Configuration 23
3.3.1.1 Configuration Reports 23
3.3.1.2 Import Configuration 24
3.3.1.3 AntiVir Servers Settings 24
3.3.1.4 Settings for an Individual AntiVir Server 29
3.3.1.5 Address Lists 34
3.3.1.6 Creating Notification Templates 41
3.3.1.7 Creating a Database Connection to an SQL-Server 46
3.3.1.8 Folder Settings 51
3.3.1.9 Utility Settings 59
3.3.2 Policy Configuration 60
3.3.2.1 Corporate Policy Example 60
3.3.2.2 Conditions 60
3.3.2.3 Job Types 61
3.3.2.4 Actions 62
3.3.2.5 Job Processing Sequence 63
3.3.3 AntiVir Monitor 63
3.3.3.1 Quarantines 64
3.3.3.2 Avira AntiVir Exchange Reports 72
4 AntiVir 73
4.2 Virus Scanning 73
4.2.1 Scanning Inbound and Outbound Messages 73
4.2.2 Scanning in the Information Store 74
4.2.3 Configuring and Enabling the AntiVir Scanner 75
4.2.4 Enabling Virus Scanning - Example 78
4.3 Virus Scan in the Information Store - Sample Job 85
4.4 File Restrictions for Attachments 93
4.4.1 By Type 93

4.4.2 By Message Size 94
4.4.3 By Type and/or Attachment Size 94
4.4.4 Configuring Fingerprints 94
4.4.5 Denying File Attachments by Type - Example 103
4.4.6 Limiting Message Size - Example 107
4.4.7 Denying Attachment Types and Sizes - Example 111
5 AntiVir Wall 116
5.2 Address Filtering 116
5.2.1 Blocking Senders and/or Recipients - Example 117
5.3 Content Filtering With Dictionaries 120
5.3.1 Setting up Dictionaries 121
5.3.2 Checking and Denying Text Contents - Example 125
5.4 Anti-Spam with the AntiVir Wall Spam Filtering Job 129
5.4.1 Definite No-Spam Criteria 131
5.4.2 Definite Spam Criteria 132
5.4.3 Practical Tips 132
5.4.4 Spam Filtering - Example 133
5.4.5 Advanced Spam Filtering 145
5.4.6 Manual Spam Filtering Configuration 149
5.5 Using SPACE for Fighting Spam 149
5.5.1 SPACE Engine Configuration 150
5.5.2 Advanced Spam Filtering Job Configuration 151
5.6 Blocking Images 152
5.7 Limiting the Number of Recipients 157

1 Getting Started

1.1 Installation on an Exchange Server

1. To install Avira AntiVir Exchange, double-click the file `antivir_exchange_server_2k_en.exe` or `antivir_exchange_server_2k7_64bit_en.exe` in the installation package.
2. Follow the Installation instructions.

   Unless you specify a different installation directory, Avira AntiVir Exchange is installed in the default directory, i.e.:

   `C:\Programme\Avira\AntiVir Exchange\ (German)`

   `C:\Program Files\Avira\AntiVir Exchange\ (English)`

Attention: *Disable any real-time or on-access scan functions of your scan engines for the `...\Avira\AntiVir Exchange\AntiVirData\` directory.*

1.2 Starting AntiVir Exchange Management Console

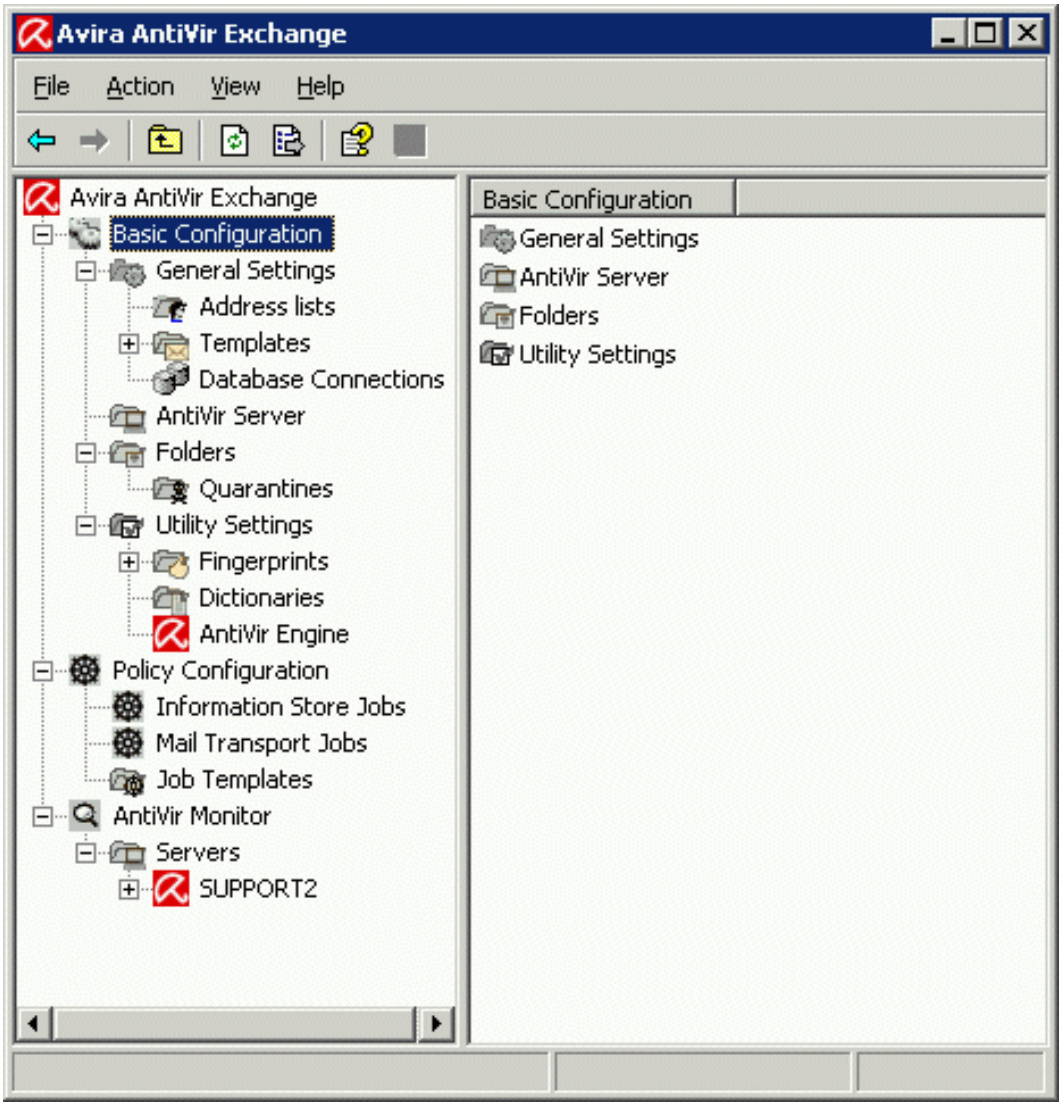
Avira AntiVir Exchange is a server product that is configured through AntiVir Exchange Management Console. For Avira AntiVir Exchange to work, the `AntiVir for Exchange` service must be running. Also refer to 3.1.2.2 Avira AntiVir Exchange Service = Enterprise Message Handler (EMH) .

1. To start the console, go to **Start - Programs - Avira - AntiVir Exchange - AntiVir Exchange Management Console**.

   Before closing the AntiVir Exchange Management Console, you are prompted to save any changes.

Note: *Pending changes are indicated by an asterisk (*) next to the top node. To save your configuration click the* ***Save*** *button. The configuration is saved in the `ConfigData.xml` file located in `\Avira\AntiVir Exchange\Config\`.*

1.3 Configuration in AntiVir Exchange Management Console



After the installation, use the AntiVir Exchange Management Console to make the required and recommended settings.

1.3.1 Required Basic Configuration Steps

Basic Configuration is used to define the valid server, e-mail addresses, shared templates and utility settings.

1. Under **Basic Configuration - General Settings - AntiVir Servers Settings** in the **Address Settings** tab, check the entries for the **Administrator(s)** and the **Internal domains**. Refer to 3.3.1.3 AntiVir Servers Settings .

1.3.2 Required Policy Configuration Steps

Use the **Policy Configuration** to define and enable selected jobs according to the company's policies.

1. Under **Job Templates**, find the template you wish to use.
2. To create a new job, select the template and drag it to the **Mail Transport Jobs** folder. Give the job a name, edit its properties, then enable the job (**Enabled**: Yes).
3. Make sure that the jobs are performed in the correct order (refer to 3.3.2.5 Job

Processing Sequence).

4. **Save** your changes. Also refer to 1.2 Starting AntiVir Exchange Management Console .

1.3.3 Recommended Basic Configuration Steps

In the **Basic Configuration**, it is recommended to define individual settings for address lists, templates, etc. However, this is not necessary for simply testing the system.

1. Configure the **Address lists** (for selections in job rules) under **General Settings**.
2. Where required, change the **Templates** under **General Settings**.
3. Under **Utility Settings**, configure any accessories required, e.g. dictionaries, fingerprints and the virus scanner.

1.3.4 Virus Scanning in Exchange Databases

Under **Policy Configuration - Information Store Jobs**, you can enter appropriate settings for each Avira AntiVir Exchange server separately.

It is not possible to create Informations Store jobs. A new Information Store job is automatically provided whenever a new server is specified.

If the server is removed, the Information Store job will also be deleted.

For further details on Information Store jobs, please refer to 4.2.2 Scanning in the Information Store .

1.4 Observing Data in AntiVir Monitor

After having saved your settings, use the **AntiVir Monitor** to monitor the operation of Avira AntiVir Exchange. With the **AntiVir Monitor**, you can view current data in real-time and manage, for example, the **Quarantine Areas** of the configured Servers.

For details refer to 3.3.3 AntiVir Monitor .

2 Installation

2.1 System Requirements

To install Avira AntiVir Exchange, your system must meet the following requirements:

- CD-ROM drive or network access
- RAM: Exchange recommendation plus additional 64 MB
- Hard disk: at least 400 MB for installation
- Microsoft .NET Framework 2.x
- Operating systems:
  - Windows 2000 Server from Service Pack 4
  - Windows 2000 Advanced Server from Service Pack 4
  - Windows Server 2003
  - Windows Server 2008.
- Exchange Server:
  - MS Exchange Server 2000 as of Service Pack 4
  - MS Exchange Server 2000 Enterprise Edition as of Service Pack 4
  - MS Exchange Server 2003
  - MS Exchange Server 2007 SP1 Update Rollup 4 Hub + Mailbox

Attention: *Disable any real-time or on-access scan functions of your scan engines for the* `...\Avira\AntiVir Exchange\AntiVirData\` *directory.*

2.2 Installation of the Virus Scanner

The AntiVir scan engine is fully preconfigured and ready for immediate use. A virus scanning job that uses AntiVir is supplied and only needs to be enabled.

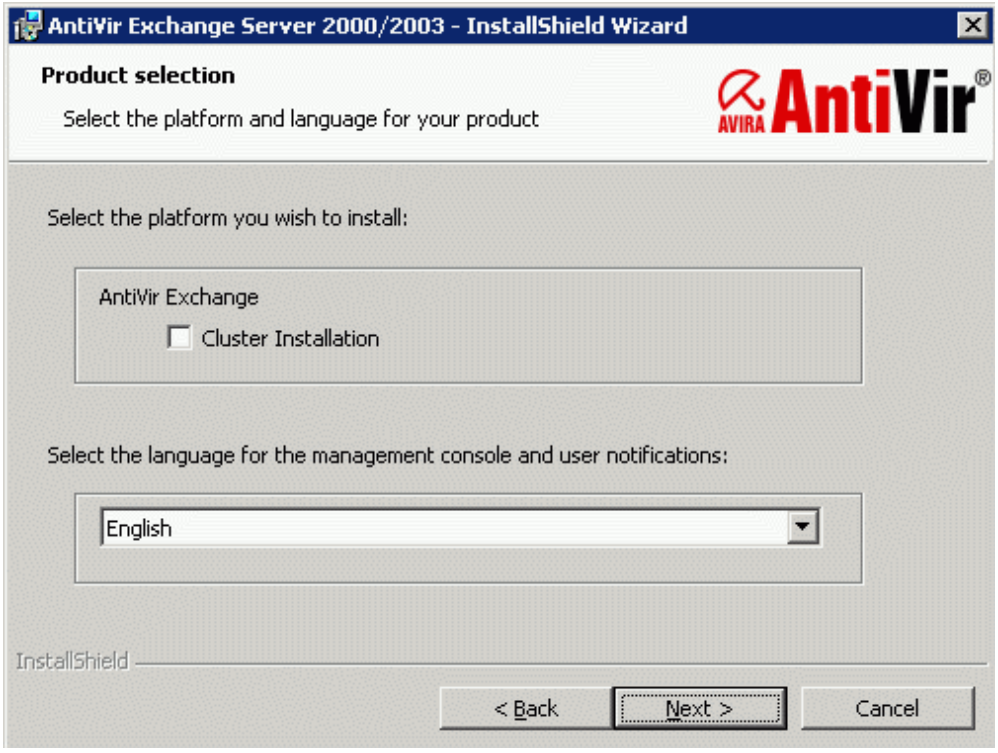
Also refer to 4.2.3 Configuring and Enabling the AntiVir Scanner .

Attention: *Disable any real-time or on-access scan functions of your scan engines for the* `...\Avira\AntiVir Exchange\AntiVirData\` *directory.*

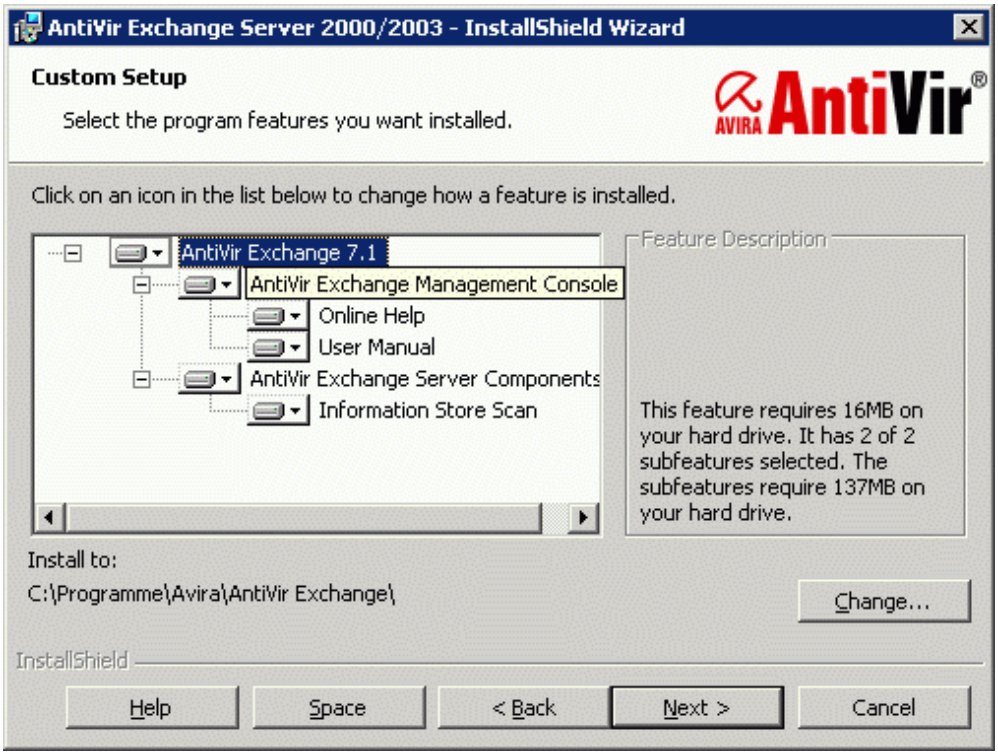
2.3 Installation of Avira AntiVir Exchange on an Exchange Server

1. From the Avira AntiVir Exchange installation package, run (double-click) the file `antivir_exchange_server_2k_en.exe` or `antivir_exchange_server_2k7_64bit_en.exe`
2. First select the **Setup language**. Then select the desired product version and language.

   The selected product language applies to the user interface and the notifications sent to the users by Avira AntiVir Exchange.

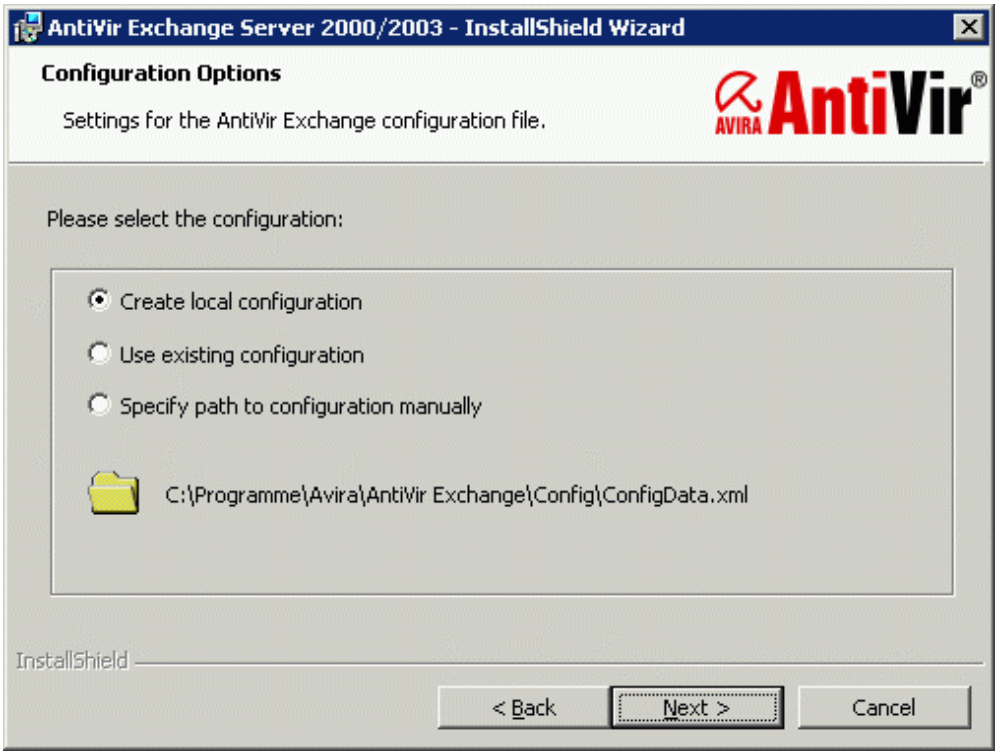


3. In the next window, accept the **License Agreement** and click **Next** to continue.
4. In the next dialogue, select the features to be installed. This selection includes all server components and the AntiVir Exchange Management Console.

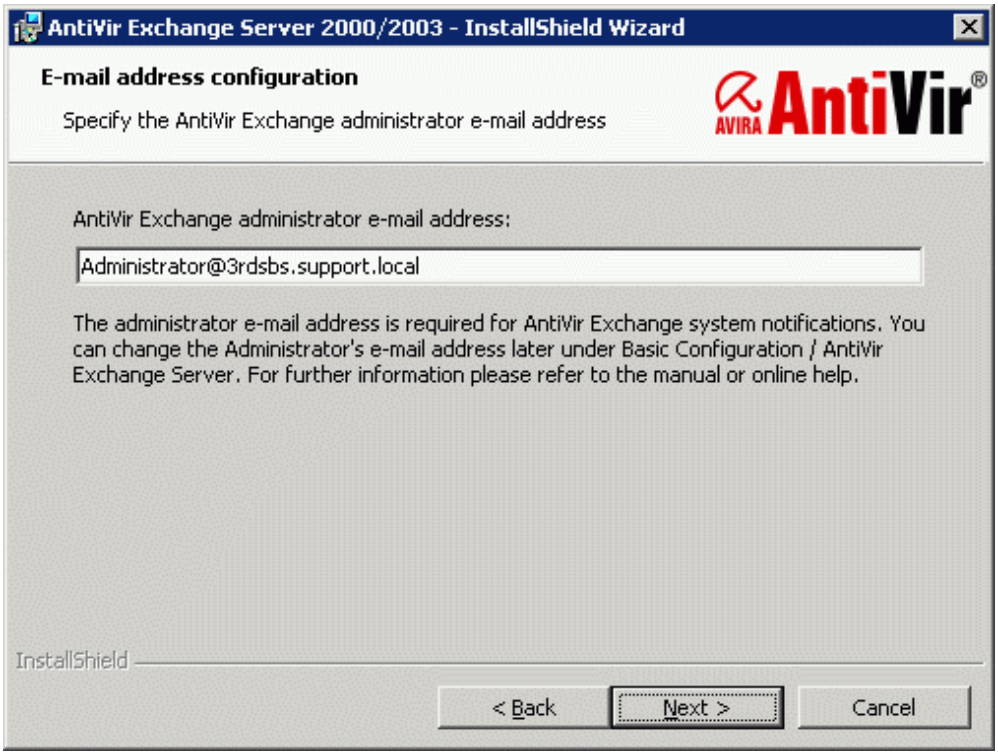

AntiVir Exchange Server 2000/2003 - InstallShield Wizard
Custom Setup
Select the program features you want installed.
AVIRA AntiVir
Click on an icon in the list below to change how a feature is installed.
AntiVir Exchange 7.1
AntiVir Exchange Management Console
Online Help
User Manual
AntiVir Exchange Server Components
Information Store Scan
Feature Description
This feature requires 16MB on your hard drive. It has 2 of 2 subfeatures selected. The subfeatures require 137MB on your hard drive.
Install to:
C:\Programme\Avira\AntiVir Exchange\
Change...
InstallShield
Help
Space
< Back
Next >
Cancel

In case another Information Store Scan application, apart from Avira AntiVir Exchange, is already running on the server, the feature will be disabled. If you wish to use Information Store Scan, the other application has to be uninstalled first.

5. Click **Next**.
6. In the next screen, you have to specify the path of the configuration file:



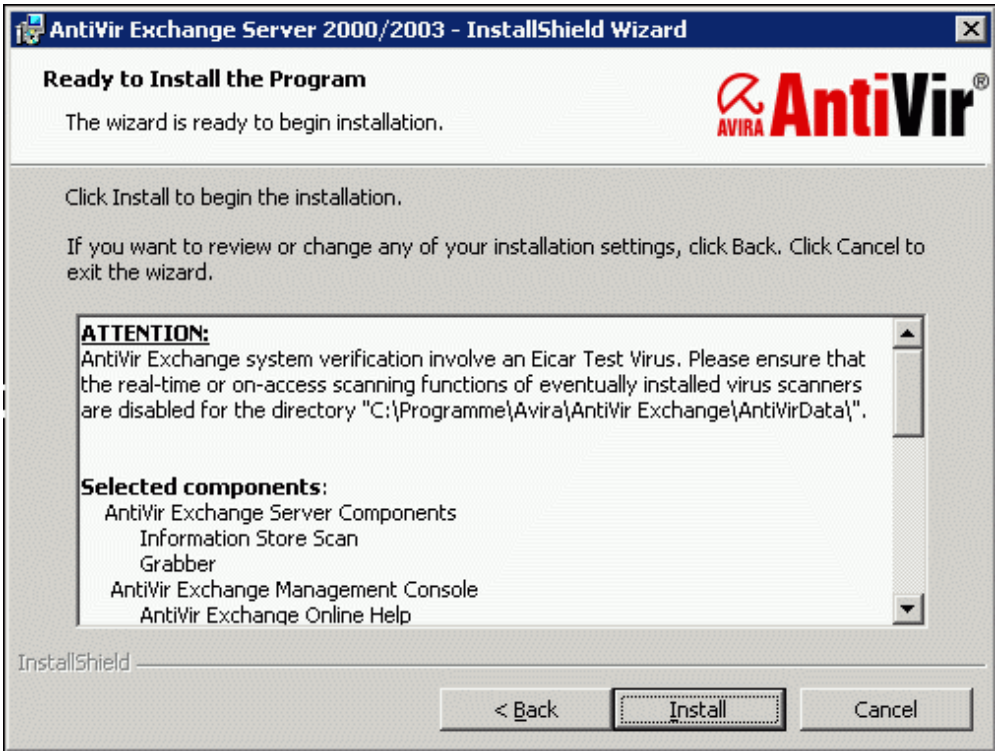
7. If you do not operate Avira AntiVir Exchange on several servers and want to work with a central configuration file for administration purposes, confirm the default setting and click **Next**.
8. In the next dialog, specify the **administrator's e-mail address**:


AntiVir Exchange Server 2000/2003 - InstallShield Wizard
E-mail address configuration
Specify the AntiVir Exchange administrator e-mail address
AntiVir
AVIRA
AntiVir Exchange administrator e-mail address:
Administrator@3rdsbs.support.local
The administrator e-mail address is required for AntiVir Exchange system notifications. You can change the Administrator's e-mail address later under Basic Configuration / AntiVir Exchange Server. For further information please refer to the manual or online help.
InstallShield
< Back
Next >
Cancel

9. If you are using a proxy server for updates, you can make the settings in the next window. Passwords are stored in clear text!

   All of the settings can later be changed in the configuration files of AntiVir.

10. A summary of your settings is now displayed:


AntiVir Exchange Server 2000/2003 - InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
AntiVir
AVIRA
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
ATTENTION:
AntiVir Exchange system verification involve an Eicar Test Virus. Please ensure that the real-time or on-access scanning functions of eventually installed virus scanners are disabled for the directory "C:\Programme\Avira\AntiVir Exchange\AntiVirData\".
Selected components:
AntiVir Exchange Server Components
Information Store Scan
Grabber
AntiVir Exchange Management Console
AntiVir Exchange Online Help
InstallShield
< Back
Install
Cancel

11. Now disable the on-access scanners for the `...\AntiVirData` directory, unless you have already done so.
12. Check your configuration settings.

    These settings will be added as standard entries to the configuration of the Avira AntiVir Exchange Server. For details refer to Avira AntiVir Exchange Server settings .

13. Follow the instructions on screen and click **Install**.

    Avira AntiVir Exchange is installed to the following directory: `<Drive>:\<default program dir.>\Avira\Avira AntiVir Exchange\`

14. Click **Finish** in the final dialog.

    Avira AntiVir Exchange is fully installed.

2.4 Uninstallation of Avira AntiVir Exchange 7

1. Go to **Start - Settings - Control Panel - Add or Remove Programs**
2. Select the **Avira AntiVir Exchange 7**
3. Click **Change** to call the Setup
4. In the Welcome window, click **Next**.
5. In the selection dialogue, click **Remove**.
6. Click **Next** and confirm with **Remove**.

   The Setup then uninstalls Avira AntiVir Exchange without removing your configuration and the Quarantine data. A decision concerning this data can be taken separately after completing the uninstallation:

AntiVir Exchange Server 2000/2003 - InstallShield Wizard
InstallShield Wizard Completed
The InstallShield Wizard has successfully uninstalled AntiVir Exchange Server 2000/2003. Click Finish to exit the wizard.
Delete all user and registry data
www.avira.com
AVIRA AntiVir
< Back
Finish
Cancel

7. Click **Finish** if you wish to keep your configuration and Quarantine data. If you want to delete all Avira AntiVir Exchange components, enable the **Delete all user and**

registry data checkbox first.

3 General

3.1 The Architecture of Avira AntiVir Exchange

Avira AntiVir Exchange consists of three main components: AntiVir Exchange Management Console, Avira AntiVir Exchange Server and Avira AntiVir Exchange configuration.

3.1.1 AntiVir Exchange Management Console

The AntiVir Exchange Management Console is the "cockpit" from where Avira AntiVir Exchange is configured and administered. It is a so-called "Snap-In" for the MMC.

The AntiVir Exchange Management Console can be used to administer individual Exchange servers with Avira AntiVir Exchange installed as well as entire "Avira AntiVir Exchange server farms". This simplifies daily administration tasks, in particular in a multi-server environment.

With the AntiVir Exchange Management Console, the Administrator has access to all configuration information needed and to the AntiVir Monitor (Quarantine) of the Avira AntiVir Exchange servers.

Two different access methods are used for configuring the system and for accessing the Quarantine.

1. Standard Windows file access

   Here, AntiVir Exchange Management Console is run directly on the Exchange server on which all components of Avira AntiVir Exchange are installed. This mode is suited for smaller systems and for managing the server locally.

2. SOAP and SSL

   The AntiVir Monitor (refer to 3.3.3 AntiVir Monitor) is accessed through SOAP and SSL using a permanently assigned communication port.

The AntiVir Exchange Management Console supports two operating modes.

1. Local Administration

   Here, the AntiVir Exchange Management Console is run directly on the Exchange server on which all components of Avira AntiVir Exchange are installed. This mode is suited for smaller systems and for managing the server locally.

2. Remote Administration

   In this case, the AntiVir Exchange Management Console is not installed on the Exchange server, but on a client.

The AntiVir Exchange Management Console can run under the following client operating systems:

- Windows 2000 Professional

- Windows 2003
- Windows XP Professional
- Windows 2008
- Windows Vista

Remote administration is suited for central administration in multi-server environments, with the AntiVir Exchange Management Console accessing one or more Exchange servers to configure and administer Avira AntiVir Exchange.

3.1.2 Avira AntiVir Exchange Server

The term Avira AntiVir Exchange Server refers to the Avira AntiVir Exchange functions and processes that are run on the Exchange server only.

The Avira AntiVir Exchange server can be installed in simple environments as well as more complex front-end/ back-end environments.

Avira AntiVir Exchange Server consists of several elements.

3.1.2.1 Grabber

The Grabber is a process ensuring that all messages, schedule queries, etc. sent, received or routed by the Exchange server are intercepted (grabbed).

The SMTP protocol is used in Microsoft Exchange for transporting e-mail, schedule queries, etc. The entire e-mail traffic is channeled through the SMTP Advanced Queue (a part of the SMTP protocol), regardless of whether the mail is internal (between mailboxes on the same server or mailbox store), inbound or outbound.

All messages must go through the Advanced Queue.The Grabber is “latched in” to this Advanced Queue. As a registered Event Sink, it monitors the mail traffic and routes all relevant information to the Avira AntiVir Exchange service – the second Avira AntiVir Exchange Server component. Each message is held there until Avira AntiVir Exchange Server has finished processing it.

Note: *Exchange-internal information, for instance replication messages, are recognized as such by the Grabber and left in the Exchange system unchanged.*

3.1.2.2 Avira AntiVir Exchange Service = Enterprise Message Handler (EMH)

As Windows service, the Avira AntiVir Exchange service is started on a permanent basis and uses all information provided by the Grabber. From then on, the subsequent processing through Avira AntiVir Exchange is entirely monitored and controlled by the Avira AntiVir Exchange service. If the Avira AntiVir Exchange service is stopped, the Avira AntiVir Exchange security functions are switched off.

The Avira AntiVir Exchange service has access to all information required, including, for instance:

- the configured Avira AntiVir Exchange jobs,
- the installed Avira AntiVir Exchange license,

- the Active Directory,
- the Avira AntiVir Exchange Quarantine

Using this information, it scans messages for viruses, identifies and quarantines spam and adds legal liability disclaimers.

After processing is complete, the Avira AntiVir Exchange service returns the e-mails to the Exchange server.

3.1.2.3 Avira AntiVir Exchange Quarantine

Virus-infected or other undesirable messages can optionally be stopped on the server to prevent them from reaching their intended recipients. These messages are instead placed in the Avira AntiVir Exchange Quarantine. Several default quarantines are set up on each Avira AntiVir Exchange server during installation. The Administrator can set up additional quarantines.

An Avira AntiVir Exchange Quarantine consists of the following:

- Quarantine directory on the Exchange server (`...\AntiVirData\Quarantine\Default Quarantine`),
- the messages copied into the Quarantine,
- Quarantine database (`LocIdxDB.mdb`).

For each quarantined e-mail, Avira AntiVir Exchange automatically creates an entry in the Quarantine database, a Microsoft Access file.

The following information is stored in that database:

- Message Subject line
- Date and time
- Message sender
- Message recipient
- E-mail sender (SMTP)
- E-mail recipient (SMTP)
- Short description of the applicable restriction
- Message size
- Name of the Avira AntiVir Exchange job that quarantined the message
- Name of the Exchange server
- Name of the e-mail file
- Processing history

When you view an Avira AntiVir Exchange Quarantine using AntiVir Exchange Management Console, the information from the Quarantine database is shown first. When you open a Quarantine entry, further information is read from the e-mail file.

For communicating with the Quarantine, Avira AntiVir Exchange uses SOAP (Simple Object Access Protocol) and SSL (Secure Socket Layer). This applies both to local access directly on the server and to access from remote Windows workstations. By default, port 8008 is used for communications. You can change this port in AntiVir Exchange Management Console (**Basic Configuration - AntiVir Server** node), but you must then also make this change in all other Avira AntiVir Exchange consoles that access the server. All stations must use the same port. SSL is used to encrypt the SOAP communications channel. The required components are included in the installation

package.

3.1.2.4 Active Directory / LDIF

Avira AntiVir Exchange does not make any changes or additions to the Active Directory. However, Avira AntiVir Exchange does read various information from the Active Directory.

When started, the Avira AntiVir Exchange service determines the available Global Catalog server, which is used, for example, for resolving addresses in distribution lists during e-mail processing.

The AntiVir Exchange Management Console uses the Active Directory to select sender/recipient conditions.

If an Active Directory is not available – for example because the corresponding ports are not open – an LDIF file can be used. This can, for example, be created through an LDAP export from an Active Directory, an Exchange 5.5 user directory or a Notes Name and Address Book (NAB).

3.1.2.5 Compressed Files and Archives: Avira AntiVir Exchange Unpacker

Files are often compressed (zipped) before being sent by e-mail. To allow compressed files to be scanned for viruses, Avira AntiVir Exchange unpacks the files before running the scan. An unpacker is automatically installed with Avira AntiVir Exchange.

The unpacker supports the following archive formats:

- ACE
- CAB
- ZIP
- Selfextracting ZIP
- ARJ
- Selfextracting ARJ
- TAR
- GZIP
- TGZ (Tape archive)
- UUE (Executable compressed ASCII archive)
- LZH (LH ARC)
- RAR
- Selfextracting RAR
- Java Archive (.jar)
- BZIP2

Note: *Archives can themselves contain further archives. By default, such recursively compressed files are decompressed to* ***a nesting depth of five levels****. All archives exceeding this nesting depth are moved to the badmail folder.*

The standard upper limit for an e-mail including unpacked files is 500 MB. Such a limit is particularly important to handle so-called ZIP of Death attacks.

The recursion depth and the space restriction can be changed in the console under **General Settings - AntiVir Servers Settings - Properties - General** tab.

3.1.3 Avira AntiVir Exchange Configuration

All information required to run Avira AntiVir Exchange is saved in the Avira AntiVir Exchange configuration file, an XML file named `ConfigData.xml`.

The structure of the `ConfigData.xml` file is similar to that of a database: various entries exist for each configuration area. Since all configuration settings are stored in a single file, the configuration can be easily distributed and backed up. If you have a problem with the configuration, you can simply send the `ConfigData.xml` file to the Avira Support team for assistance.

The configuration settings are needed by both the Avira AntiVir Exchange Server and the AntiVir Exchange Management Console. The Avira AntiVir Exchange server needs it, for example, to be informed of the Avira AntiVir Exchange jobs to be carried out. To make changes to the configuration with the console, the console must be able to access the `ConfigData.xml` file. The configuration file can be placed both in a local directory and on a shared network path. The Avira AntiVir Exchange configuration used by the AntiVir Exchange Management Console and the Avira AntiVir Exchange Server is specified through an entry in the Registry. The path to the configuration file can be entered in the format `C:\.....` or as UNC path (`\\Servername\Share\ConfigData.xml`). If the Avira AntiVir Exchange configuration file specified is not available, Avira AntiVir Exchange uses the "last known good" configuration, which is logged in the Windows Events Log.

The last known good configuration is saved locally for each server and is updated whenever the Avira AntiVir Exchange configuration is changed and access from the Avira AntiVir Exchange configuration file to the last know good configuration is possible.

Tip: *To open a non-standard configuration with the Management Console, you must specify the file with a special parameter. Run the `Avira.msc` file with the parameter `config` and the desired configuration file, e.g.:*

```
"C:\Program Files\Avira\AntiVir Exchange\Avira.msc" config
"C:\OtherFolder\Directory\ConfigData.xml"
```

You can also specify a UNC path here.

For detailed instructions for customizing the Avira AntiVir Exchange configuration, refer to 1.3 Configuration in AntiVir Exchange Management Console .

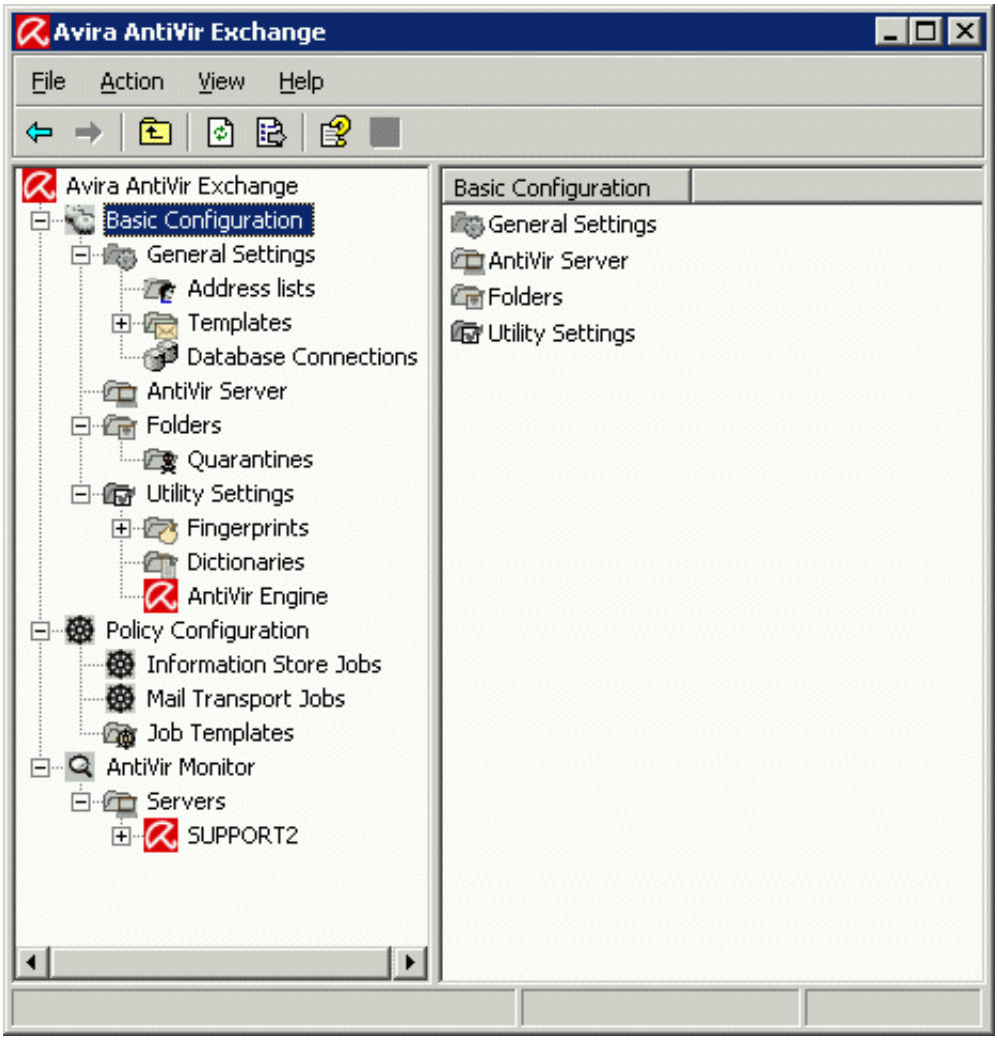
The sequence is as follows:

1. An e-mail message arrives at the mail server.
2. The e-mail is intercepted from the SMTP Advanced Queue by the Grabber.
3. The Enterprise Message Handler (EMH) [= Avira AntiVir Exchange Service] fetches the mail for processing.
4. According to the configuration settings, the EMH checks whether or not the e-mail is to be processed by Avira AntiVir Exchange.
5. Messages to be processed are dealt with as specified in the configuration settings (jobs by priority).
6. When processing is complete, the EMH releases the e-mail and, if applicable, modifies the e-mail as configured.

3.2 User Interface

1. Start Avira AntiVir Exchange
2. Select **Basic Configuration**, **Policy Configuration** or **AntiVir Monitor** in the left column.

   The window on the right then shows the corresponding subfolders.



3. To view the **Online Help**, click on the **Help** button in the toolbar or select **Help** from the **Action** menu.

3.2.1 Toolbar

	Previous
	Next
	Up one level
	Properties of the selected item
	Update view
	Export list
	Help

	Save
	Move up one position
	Move down one position
	Enable job
	Disable job
	New item
	Set filter in Quarantine/ badmail
	Disable filter in Quarantine/ badmail

3.2.2 Icons

	Avira AntiVir Exchange Start console and logo.
	Basic Configuration for general settings for all modules.
	Node for **Global Settings**.
	The **Address lists** folder.
	An individual **Avira AntiVir Exchange address list** (red collar). Included by default in Avira AntiVir Exchange, cannot be edited.
	An individual **user-defined address list** (yellow collar). Created by the user and to be configured under **Properties**.
	The **Notification Templates** folder, which contains the individual templates notification for each job type and recipient.
	An individual **notification template**; to be configured under **Properties**.
	Icon for **Database Connections**.
	Icon for an individual **database connection**, to be configured under **Properties**.
	A list of all Avira AntiVir Exchange servers, in which you can add, remove and configure servers. The common server properties are defined under **General Settings - AntiVir Servers Settings**. Alternatively, right-click **AntiVir Server - Properties**. This includes the default e-mail addresses and the internal domain(s).
	General **AntiVir Servers Settings** under the **General Settings** node in the window on the right.
	An individual AntiVir server; to be configured under **Properties**.
	Folder Settings and **Utility Settings**. Folder Settings includes the **quarantines**, while Utility Settings covers all **add-ons**, such as virus scanner, fingerprints,

	dictionaries.
	The **Quarantine** folder structure, which contains all Quarantine folders.
	An individual Quarantine folder; to be configured under **Properties**.
	The **Fingerprints** folder.
	A logically linked **fingerprint group**.
	An individual **fingerprint**; to be configured under **Properties**.
	The folder for the **Dictionaries** used for content filtering.
	An individual **dictionary**; to be configured under **Properties**.
	The AntiVir scan engine; to be configured under **Properties**.
	Policy Configuration for configuring individual jobs according to the company policy.
	Folder for **Job Templates**; includes sample jobs for each job type.
	The template of an AntiVir job or AntiVir Wall job, to be configured under **Properties**.
	An active job, to be configured under **Properties**.
	An inactive job, to be configured under **Properties**.
	The **AntiVir Monitor** for viewing all Quarantine Areas on each available server. The Quarantine Areas contain the copies of original messages, including attachments.
	The **Quarantine Areas** folder viewing the original messages. Detailed information is available for each e-mail.
	A single quarantined object.
	An invalid quarantined object.
	A resent quarantined object.
	Information Store Quarantine object.
	Time and weekday of **Quarantine** maintenance.
	Folder for **AntiVir Reports** supplied with Avira AntiVir Exchange.
	Individual **AntiVir report**.

3.3 Configuration in AntiVir Exchange Management Console

The AntiVir Exchange Management Console window consists of three sections: Basic

Configuration, Policy Configuration and Avira AntiVir Exchange Monitor.

3.3.1 Basic Configuration

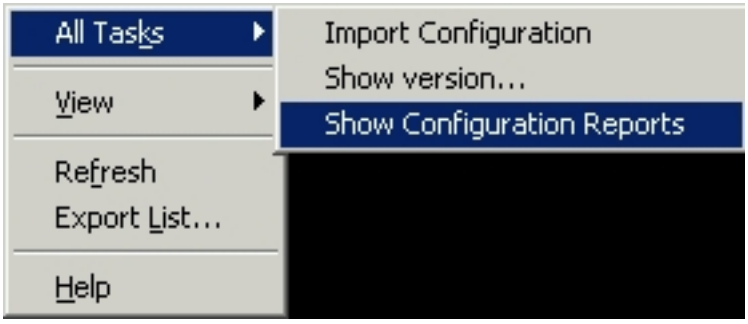
The Basic Configuration is used for general settings and the essential basic settings of the modules.

- General settings, such as:
  - address lists
  - templates
  - Avira AntiVir Exchange servers
- Folders (such as Quarantines)
- Utilities:
  - dictionaries for content checking
  - fingerprints for blocking attachments
  - AntiVir Engine

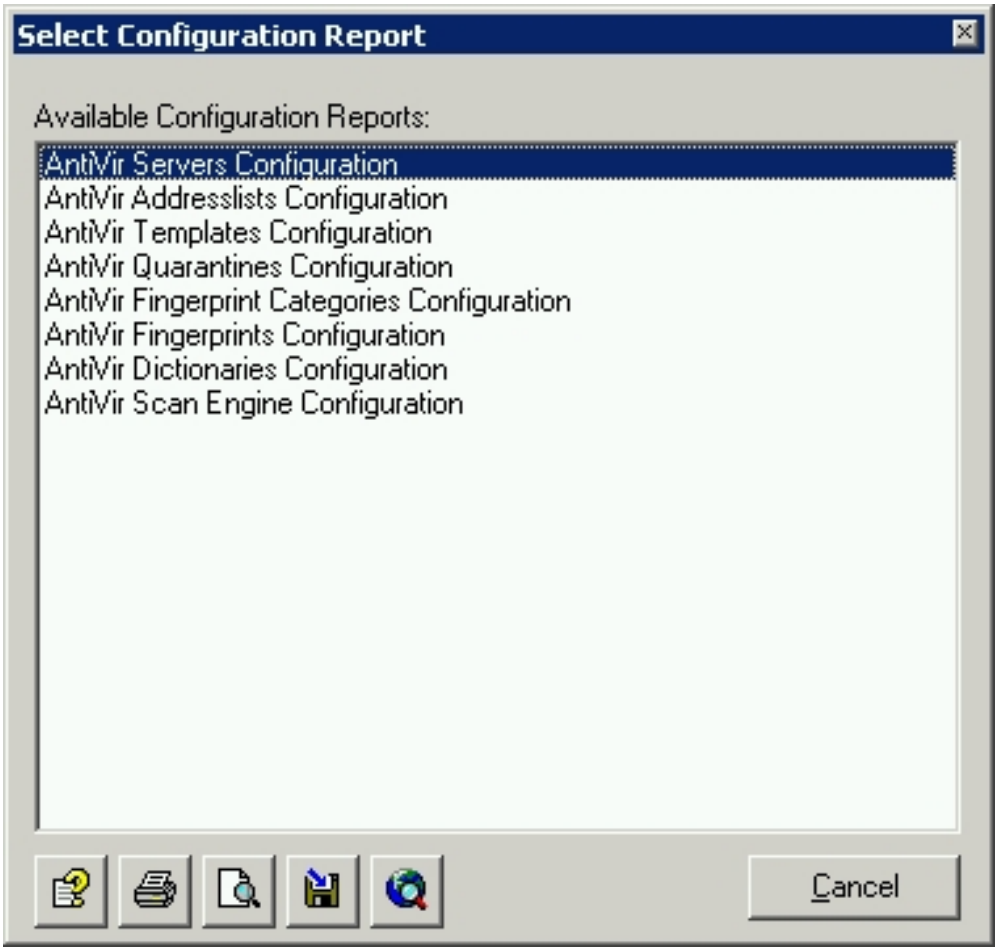
3.3.1.1 Configuration Reports

The configuration reports provide an overview of the current configuration:

1. Right-click on **Basic Configuration** and select **All tasks - Show Configuration Reports**.



2. Click on the desired report:



3. Click on **Display report**:

   The report is opened as HTML file in the browser.
4. Click **Preview Report** for a preview of the printed report.
5. Click **Save Report** to save the selected report as HTML file.

3.3.1.2 Import Configuration

Attention: *Before you update a Basic Configuration object, make a backup copy of the existing object. The new version replaces the old one, overwriting any user-defined settings.*

To update any elements and items (such as dictionaries and fingerprints) with a new version:

1. Select **Basic Configuration - All Tasks - Import Configuration**
2. Select the appropriate XML file provided by Avira for update purposes

Attention: *This function updates only individual jobs, not the complete configuration (`ConfigData.xml`).*

3.3.1.3 AntiVir Servers Settings

The AntiVir Servers Settings option is used to configure the standard settings for all Avira

AntiVir Exchange servers. Additionally, each server can be configured individually; for details refer to 3.3.1.4 Settings for an Individual AntiVir Server .

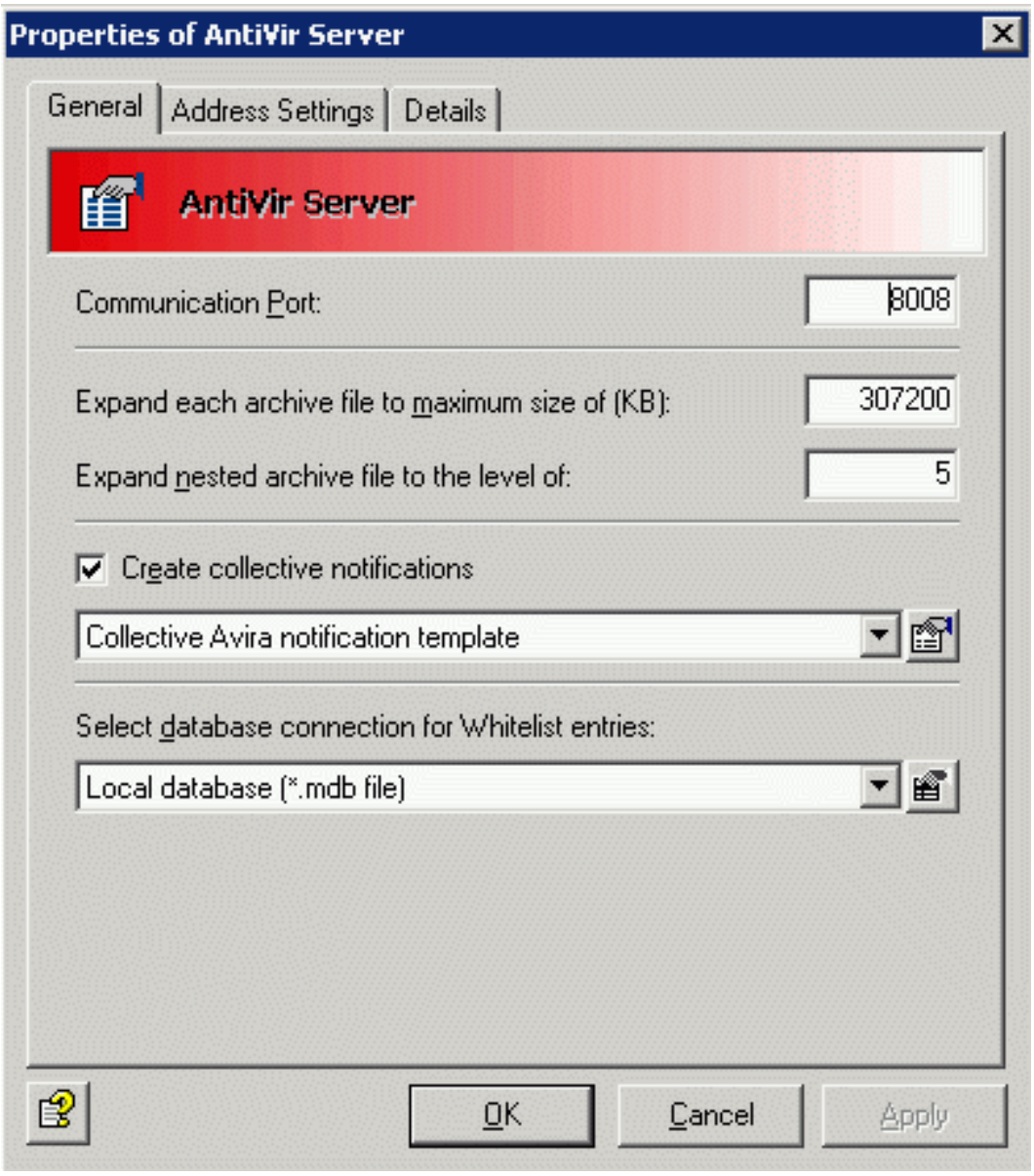
1. Select **Basic Configuration - General Settings**
2. To open the **Properties**:
   a. In the right window, right-click on **AntiVir Servers Settings** and select **Properties**.
   b. Or open the **Properties** with a double-click on **AntiVir Servers Settings**.
   c. Or in the left window section under **Basic Configuration**, right-click on **AntiVir Server** and select **Properties**.

Packed Files and AntiVir Monitor

The settings on the **General** tab set the maximum size of unpacked files on the hard disk and the maximum recursion depth for archives. Whenever an e-mail exceeds one of these values, it is moved to the **BADMAIL** area.

Attention: *Be sure to use a correct setting for the communication port for AntiVir Monitor. Otherwise, communication with the servers will be impossible.*

Usually, port 8008 is used (also entered as default port during installation). The values specified here apply to all servers.



In this context, also read the description on allocating rights and security settings under 3.3.3 AntiVir Monitor .

Collective Notification

As a general rule, each job can be configured so that when a specific event occurs, the recipients, senders and/or administrators are informed of this event (**Actions** tab).

If several events occur for an e-mail, the Avira AntiVir Exchange servers are not configured (by default) to send separate notifications for each event. Instead, all notifications are combined to a single collective notification, i.e. the recipients receive a single notification mail with a list of all events that have occurred.

The template used is under **Collective Notifications Templates**. You can change this template or create new templates.

Note: *If you prefer to send individual e-mail notifications for each event, select* ***General Settings - AntiVir Servers Settings - Properties - General*** *tab and*

*disable the **Create collective notifications** option.*

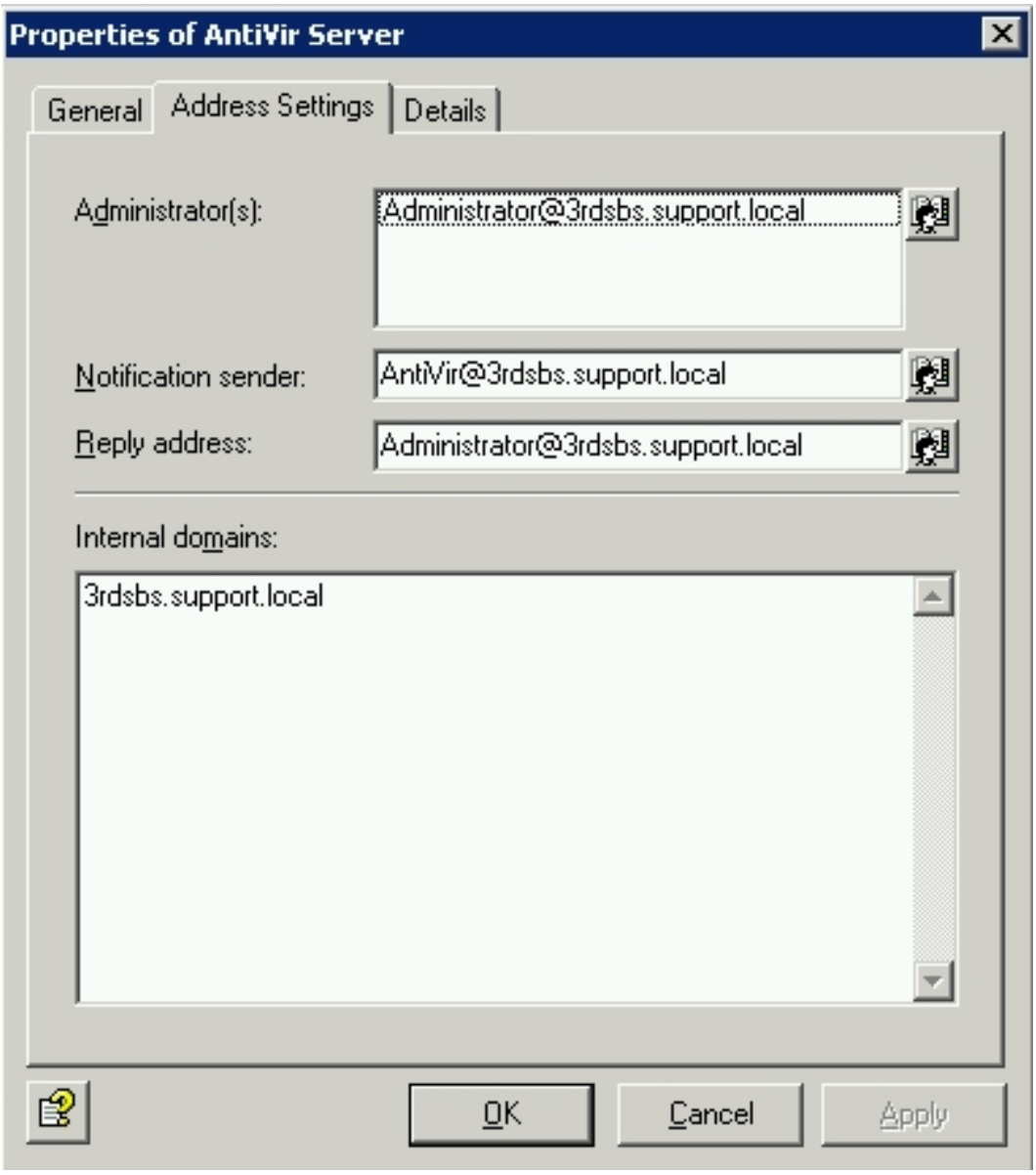
Central Whitelists

In multi-server environments each server involved creates its own user whitelists. Thus, without server synchronization, each user is provided with a separate whitelist for each of the servers, which all need to be maintained individually. In order to manage these whitelists centrally and simplify administration, you can set up a Microsoft SQL server instead of the standard local database based on the Microsoft Jet Engine. This Microsoft SQL server will write the information for all Avira AntiVir Exchange servers involved to a central SQL database.

To create a central user whitelist, you need to configure a database connection between the SQL server and the Avira AntiVir Exchange Server (**Basic Configuration - Database Connections**). Once the connection has been established, select the appropriate configuration in the **Select database connection for Whitelist entries** field, under **AntiVir Servers Settings - General** tab.

Definition of e-mail addresses and internal domains

Avira AntiVir Exchange requires a number of basic settings concerning the mail domain of the mails processed. During installation, the e-mail address of the Avira AntiVir Exchange Administrator specified is used for the following Avira AntiVir Exchange basic settings:



- **Administrator(s)**: The Avira AntiVir Exchange Administrator addresses entered in this field will receive important status notifications on the installation as well as the configured Administrator notifications. As default, the installation enters the Administrator address prompted for.
- **Notification sender:** The sender shown in the Avira AntiVir Exchange notifications. As default, the installation enters Avira AntiVir Exchange with the mail domain of the Administrator address prompted for.
- **Reply address:** The recipient stored in the Avira AntiVir Exchange notifications of replies to these notifications. As default value, the installation program enters the Administrator address prompted for.
- **Internal domains:** The mail domains entered in this field are considered as internal mail domains, all others as external ones. This setting is used to enable the Avira AntiVir Exchange rule engine to identify incoming and outgoing mails through the sender and recipient addresses. For instance, a spam filter job will only apply to incoming mails, while a trailer is not to be added to an incoming mail.

Multiple domains are separated by Carriage Return. Subdomains are automatically included, when the main domain is preceded by a "*" wildcard, e.g. `*.domain.com`. As default, the installation enters the mail domain of the Administrator address prompted for.

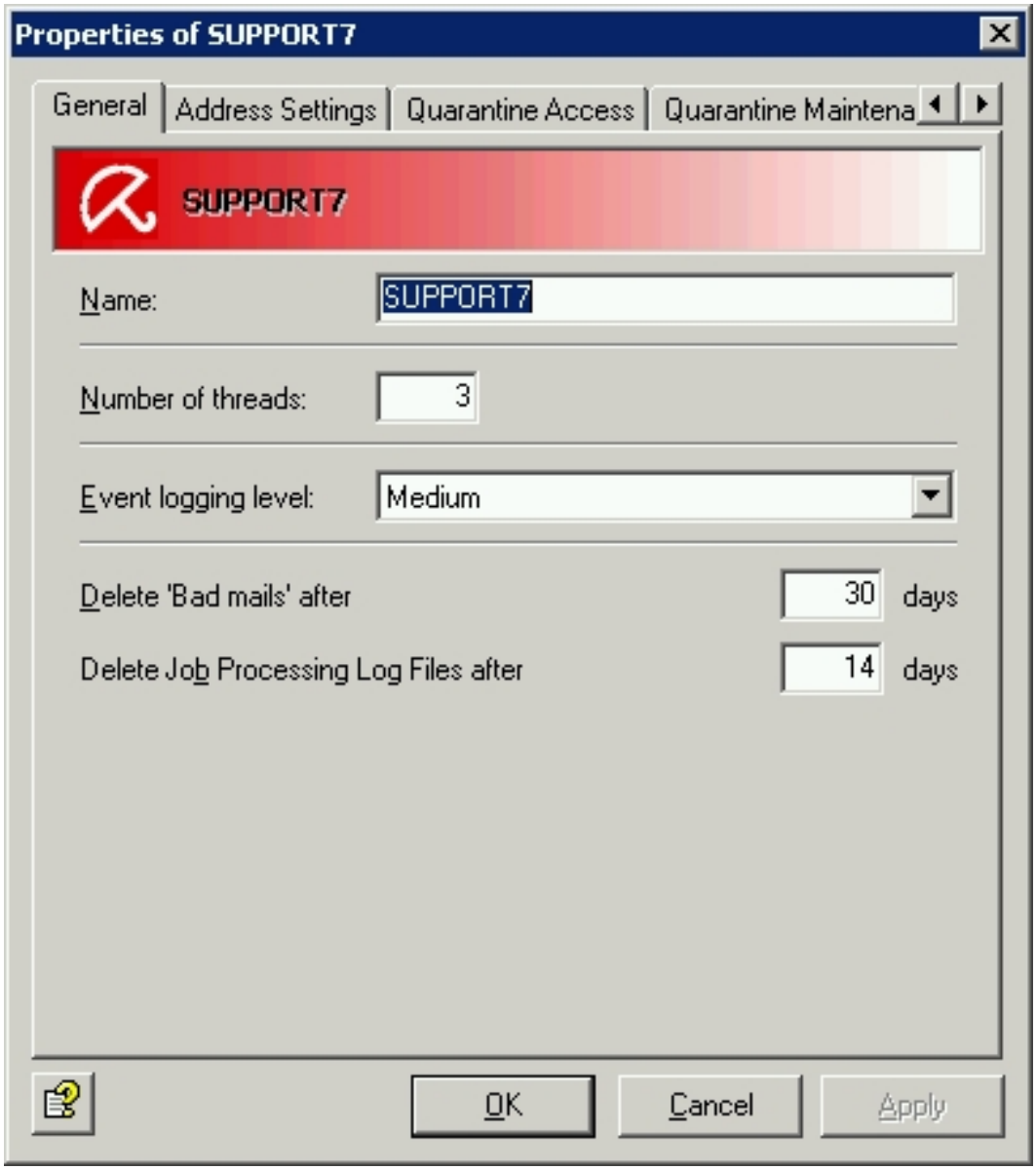
These entries apply to all Avira AntiVir Exchange servers. The settings can be changed at any time in the same window.

3.3.1.4 Settings for an Individual AntiVir Server

Select **Basic Configuration - AntiVir Server** and in the right window double-click the required server to view its properties.

To define a new server, right-click **AntiVir Servers - New - AntiVir Server** and edit its **Properties**.

General Server Settings



1. Enter the **Name** of the Exchange server.

   During the installation, the current Exchange server is automatically entered as the internal domain.

2. Set the maximum number of e-mails processed simultaneously by Avira AntiVir Exchange in the **Number of threads** field.

   A reasonable maximum depends on the capacity and performance of your server.

3. Select the **Event logging level** for the Event Log.

   You can view this log with the Event Viewer (Windows Event Log). The options range from **None** to **Maximum**.

4. Set the number of days the mails are to remain in the BADMAIL Quarantine.

   When this period expires, the mails are automatically deleted.

5. Set the number of days after which a job processing log in the Log folder is to be deleted.

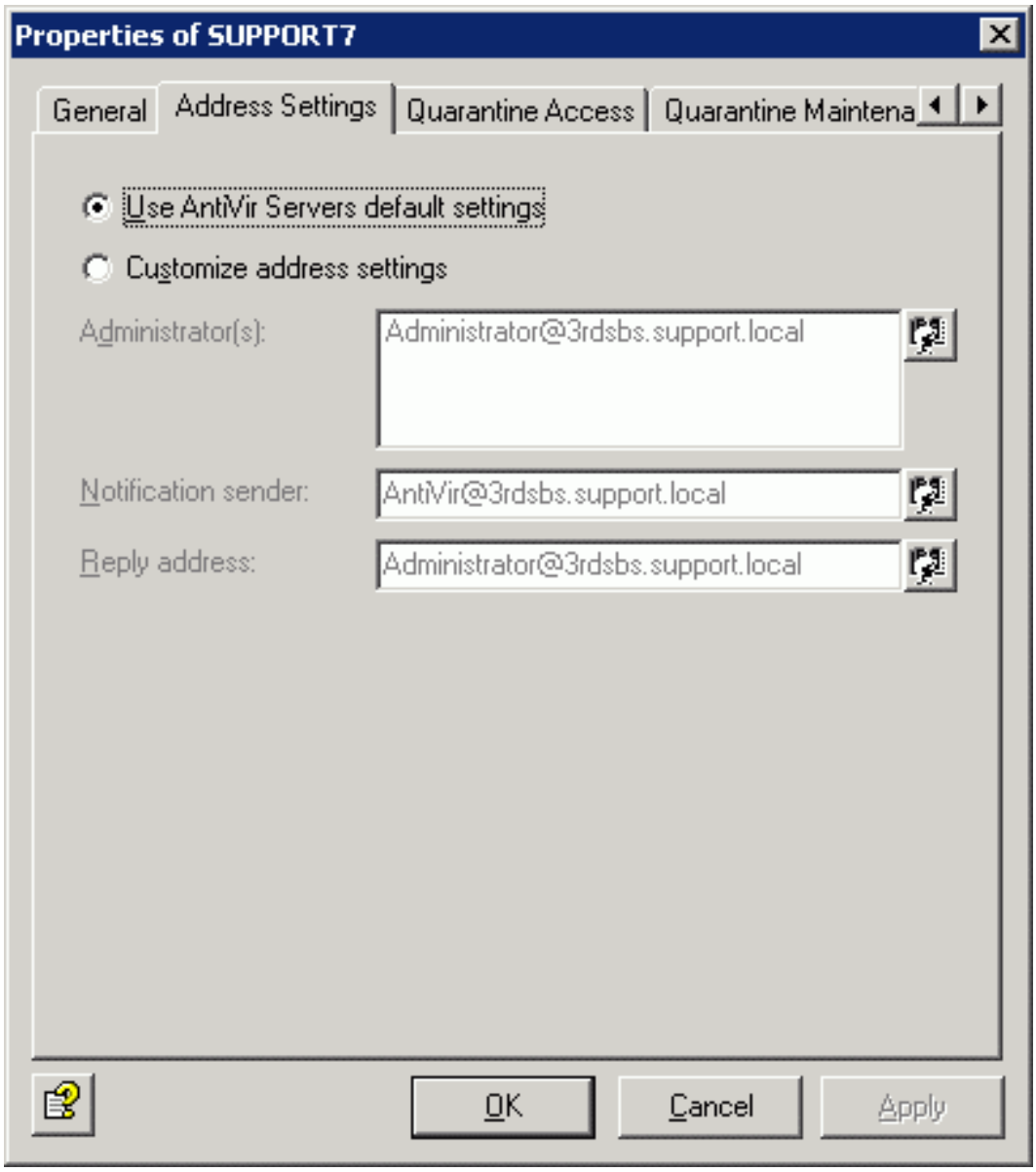
Tip: *To be able to access a newly created server in the AntiVir Monitor, refresh the*

*view in the Monitor (right-click on **AntiVir Monitor - Refresh** or click on the **Refresh** icon in the toolbar).*

Individual E-mail Addresses for an AntiVir Server

Both the user-defined and default installation settings in the **Properties** for all Avira AntiVir Exchange Servers are copied to each individual server. These are the **AntiVir Servers default settings**.

To specify different settings for a specific server, enable the **Customize address settings** option and enter the new addresses in the appropriate fields.



User-specific Access to Quarantine

With Avira AntiVir Exchange, users can access their quarantined messages themselves.

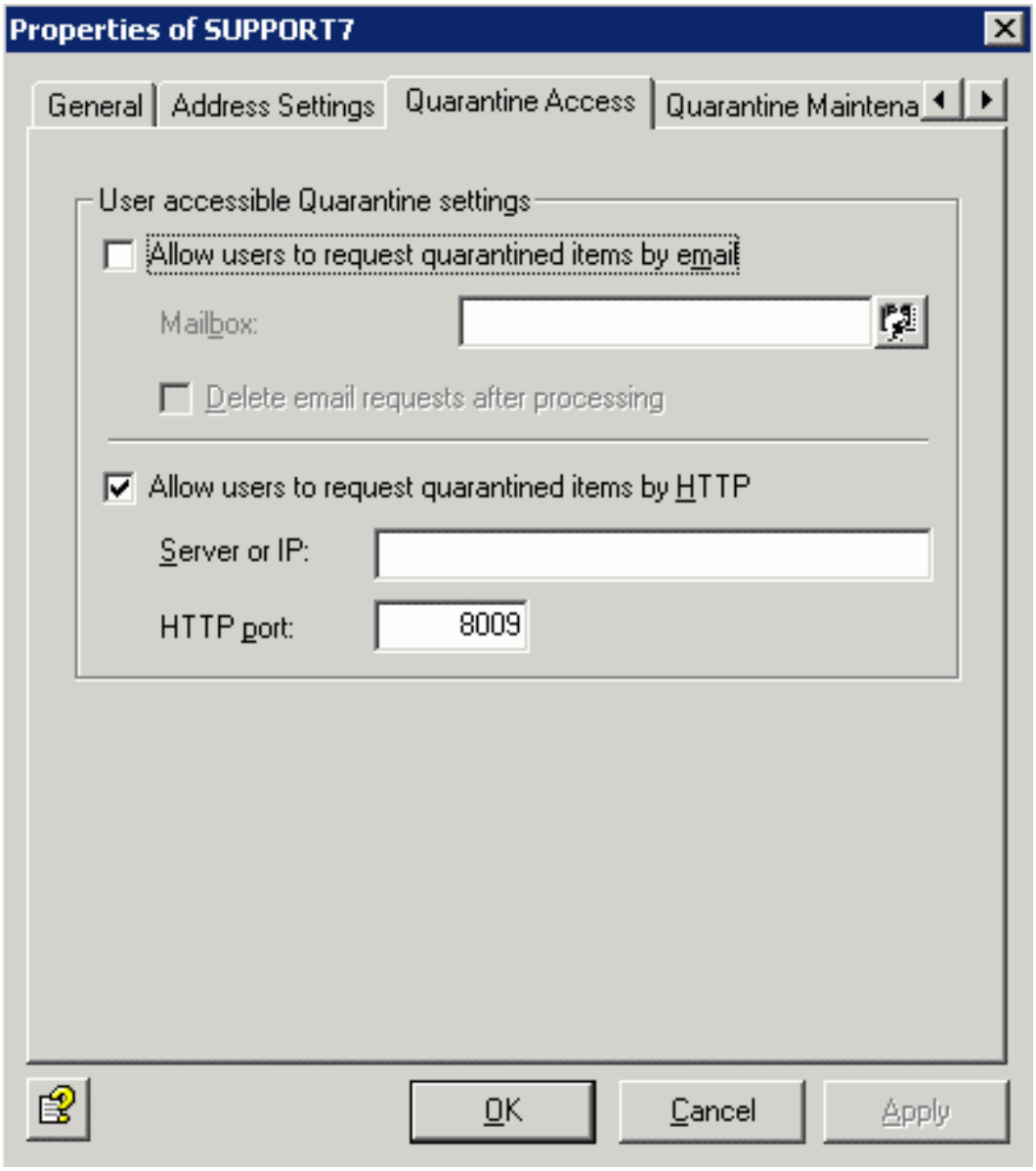
For each Quarantine, you can specify individual access rules for messages and users.

This function is especially useful for spam filtering, i.e. for the spam quarantines. It also helps to reduce the administrator's workload by allowing users to forward quarantined messages to their inboxes.

For each server you can specify whether and how users can access their quarantined mail. The user receives a summary report on quarantined mails, clicks on the corresponding action for the selected mail and, by doing so, sends a request.

These actions are configured individually for each Quarantine and include **Request** (delivery to the recipient of the summary notification), **Release** (delivery to all recipients) and/or **Remove** (mail marked for deletion in the Quarantine). The user gets access through a mail request or a HTTP request.

Select the Quarantine access tab:



Allow users to request quarantined items by email: Quarantine queries are started by a mail request. This message is generated automatically when the user clicks the action link for a quarantined message in the summary report and is sent to the e-mail address

entered in the **Mailbox** field on this tab.

A precondition is that the e-mail address exists and that the mail is sent through the server on which Avira AntiVir Exchange (and the applicable quarantines!) are installed.

We recommend that you set up the mailbox on the same server. The message content is read out, thereby triggering the action requested by the user. Avira AntiVir Exchange recognizes request messages through:

1. the e-mail address (specified in the **Mailbox** field),
2. the keyword for a user request in the message (User Request)

Finally, the request message is placed in the specified mailbox.

To delete request messages once they have been processed, check the **Delete request mails after processing** option.

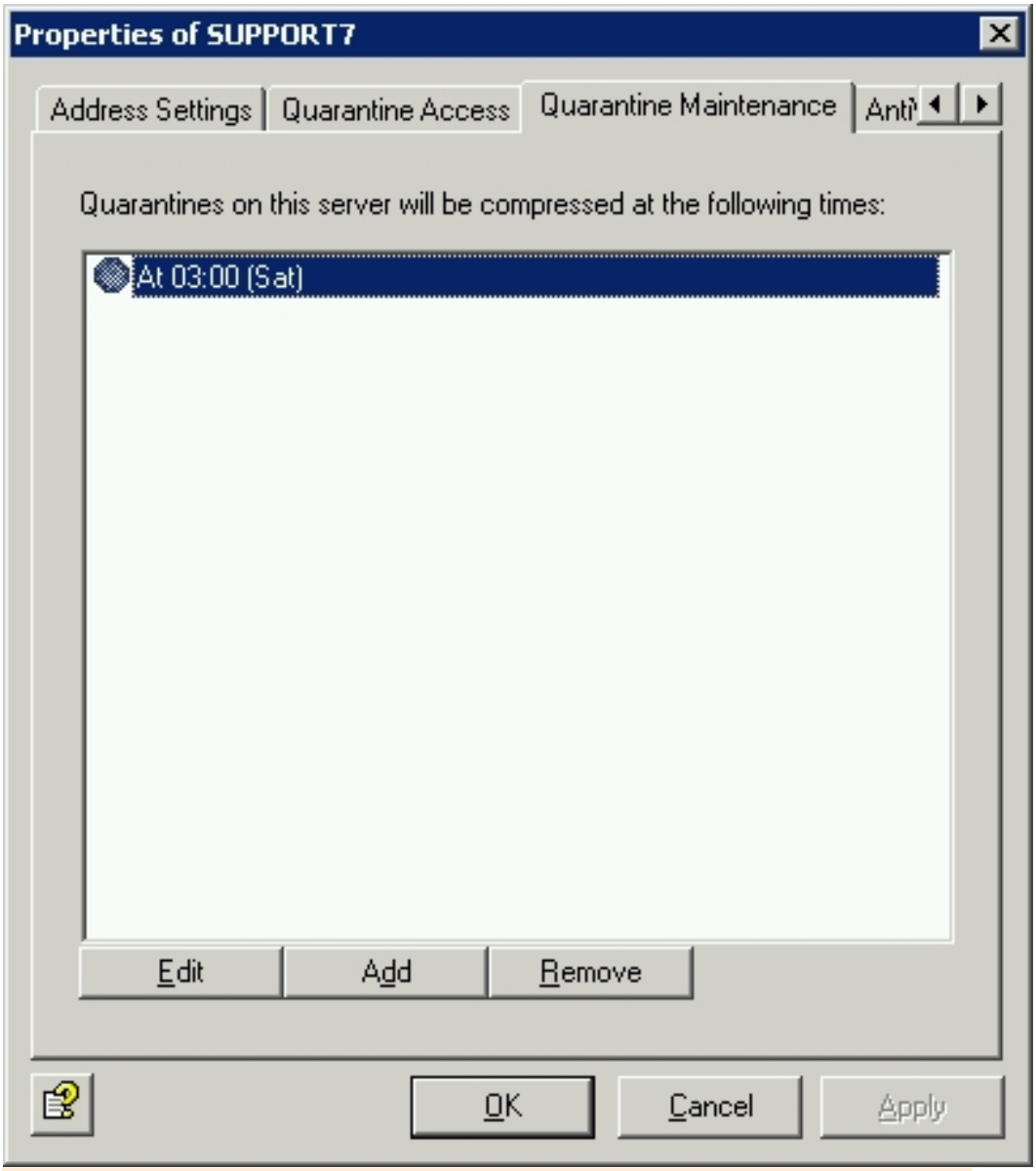
Allow users to request quarantined items by HTTP: Quarantine queries are started by an HTTP request. When the user clicks the required action, the default Web browser opens. The user is notified that the inquiry is being processed. The precondition for this inquiry is a free port. The default port is 8009.

Attention: *The browser always displays the same feedback message (`OK_Response.html` in the `Avira\ AntiVir Exchange\AppData\` directory). If the requested message no longer exists (for example because it has been deleted from the Quarantine), the user is not notified.*

Quarantine Maintenance

Use this tab to specify the time at which the Quarantine on the servers is to be purged. This deletes all messages marked for deletion to make space for newer messages.

The default setting is each Saturday at 03:00 a.m. If you wish to modify the time and/or the purge period, click **Edit** and enter the selected time.



Tip: *If necessary, you can also purge quarantines manually. To do so, right-click on the quarantine under* ***AntiVir Monitor - Servers - server_name - Quarantine Areas*** *and select* ***All Tasks - Compress Quarantine****.*

View a List of All Jobs

The **AntiVir Jobs** tab provides a list of all jobs defined on this server.

To edit a job on the server, select the job properties.

3.3.1.5 Address Lists

Under **Address lists**, you can create your own address lists to be selected for individual jobs. The available addresses are taken from the Active Directory.

Creating, editing or deleting address lists

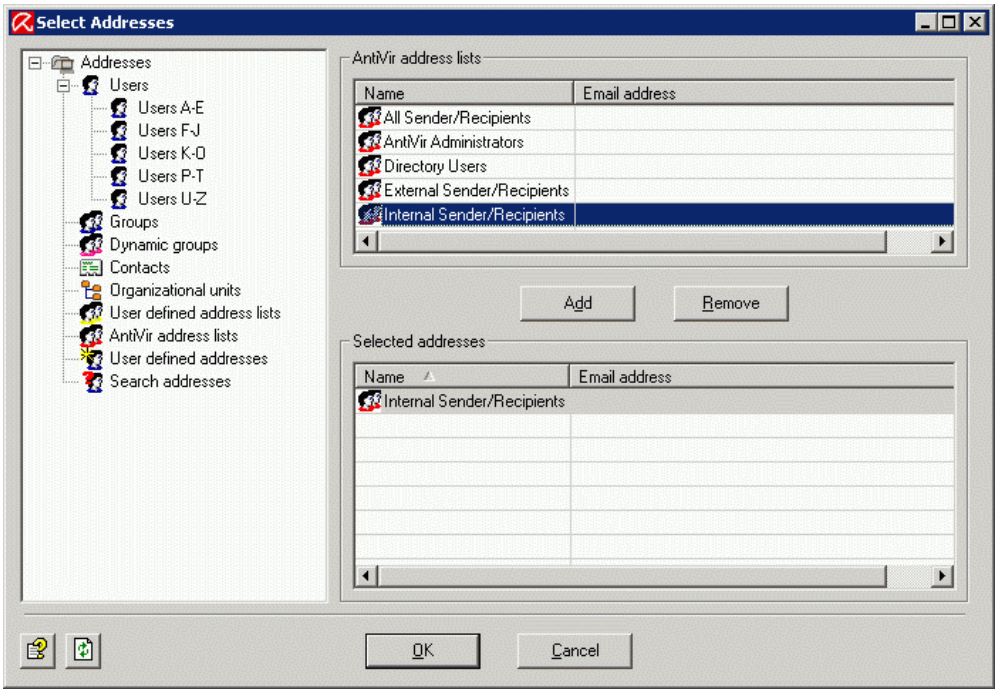
1. Go to **Basic Configuration - General Settings**

2. Click **Address lists**.
3. Right-click and select **New - Address list** from the context menu.
4. Enter a meaningful name for the address list.
5. Click the **Select members** icon: .
6. In the window that opens, select the addresses to be added and click **Add**.

   To add your own addresses to the address list, enter them in the input field. You can use the * (asterisk) and ? (question mark) wildcards. It is also possible to enter formally invalid e-mail addresses such as `info@domain`. Press **Enter** before each new entry.

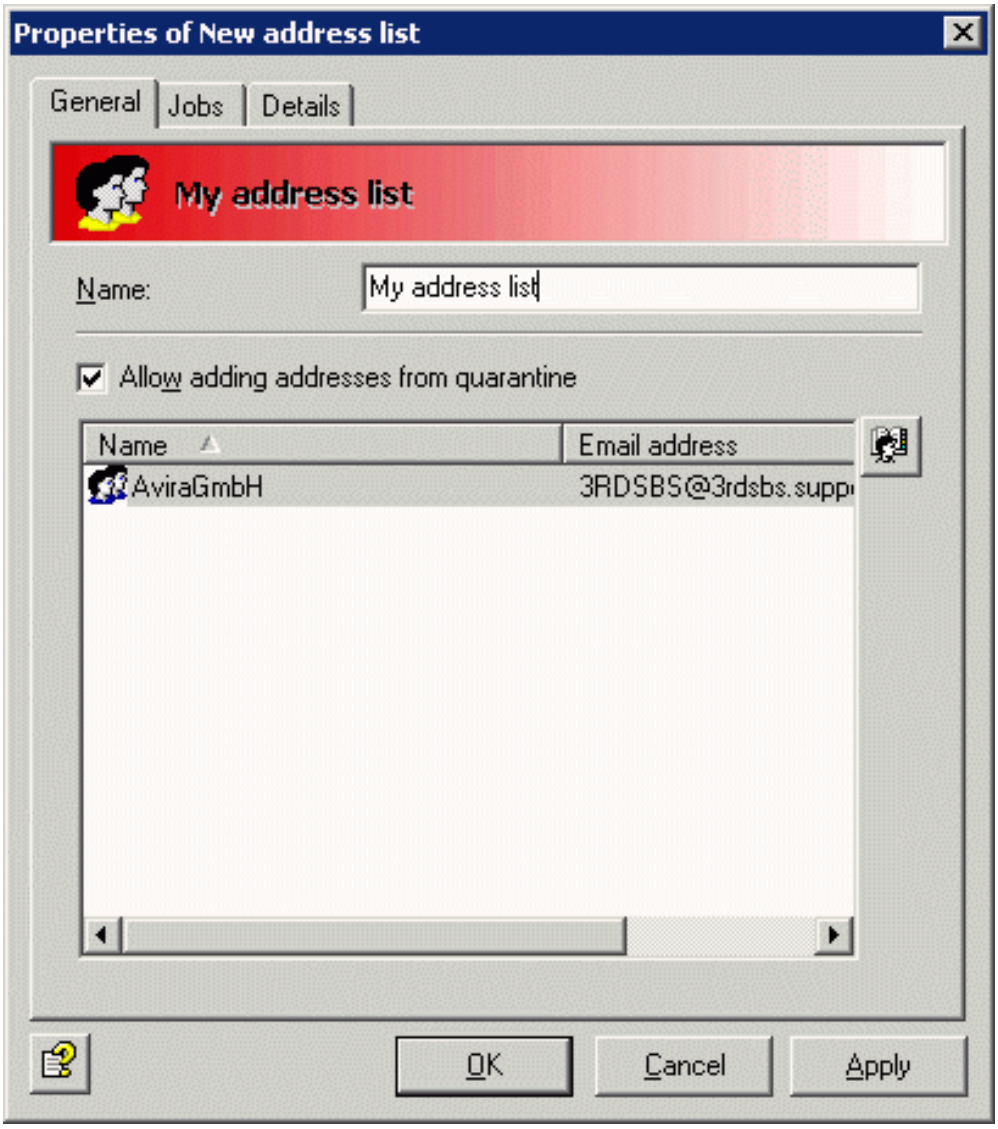
   To search for an entry in a large list of custom addresses, click on the **Search** icon . This text search function is also available for dictionaries.

   To remove an entry from the list, select it and click **Remove**.



7. Click **OK**.

   Your address list should now look like this:



8. **Allow adding addresses from quarantine**

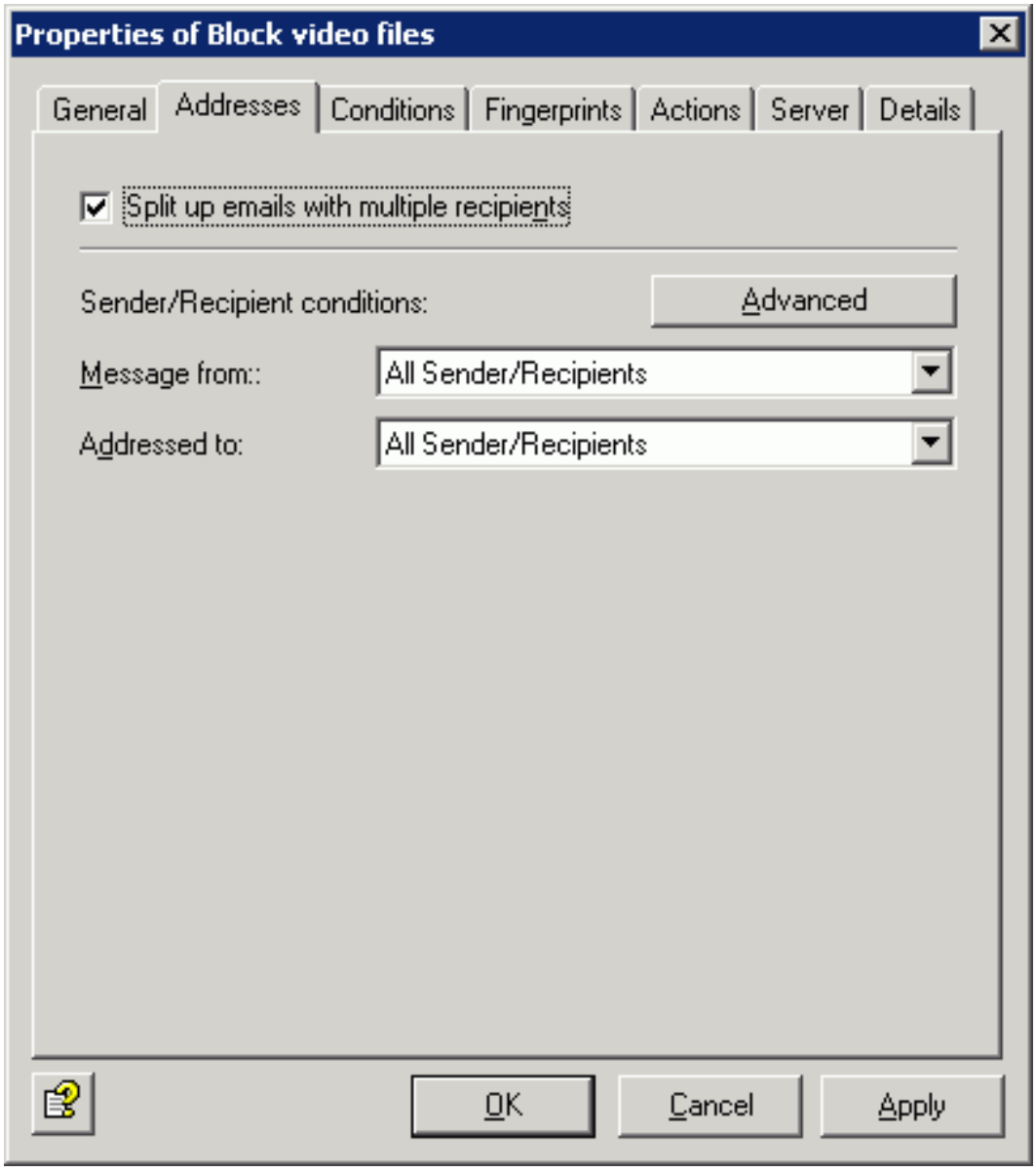
   Use this option to specify whether or not addresses from quarantined messages can be directly added to this address list. When checked, you can add the quarantined mail's sender address to various address lists with the **Add** button in 3.3.3 AntiVir Monitor . By default, the following address lists are enabled for direct access:

   - Anti-Spam: Blacklist
   - Anti-Spam: Newsletter Blacklist
   - Anti-Spam: Newsletter Whitelist
   - Anti-Spam: Whitelist

9. Click **OK** again.
10. To delete an address list, click **Address lists**, right-click the list and select **Delete** from the context menu.

Using and Handling Addresses Within a Job

In each job, the **Addresses** tab allows to set the users for whom a job is valid. Most of the current application cases can be set with options available:



Set whether the job is to be valid for all users or restricted to internal or external users. This selection is available for senders and recipients.

Note: *Both conditions in the* ***Message from*** *and* ***Addressed to*** *fields must come true for an action to be triggered (logical AND!).*

Split up emails with multiple recipients: If a message is addressed to several recipients and one or more of these are entered in an address filtering job, the message is split into two e-mails: one for the recipients specified in the address filtering job and one for the remaining recipients. Only the message with the specified recipients is processed by the job. The message is not split if no address filtering was defined for the recipients! Note that splitting messages affects the performance of your server.

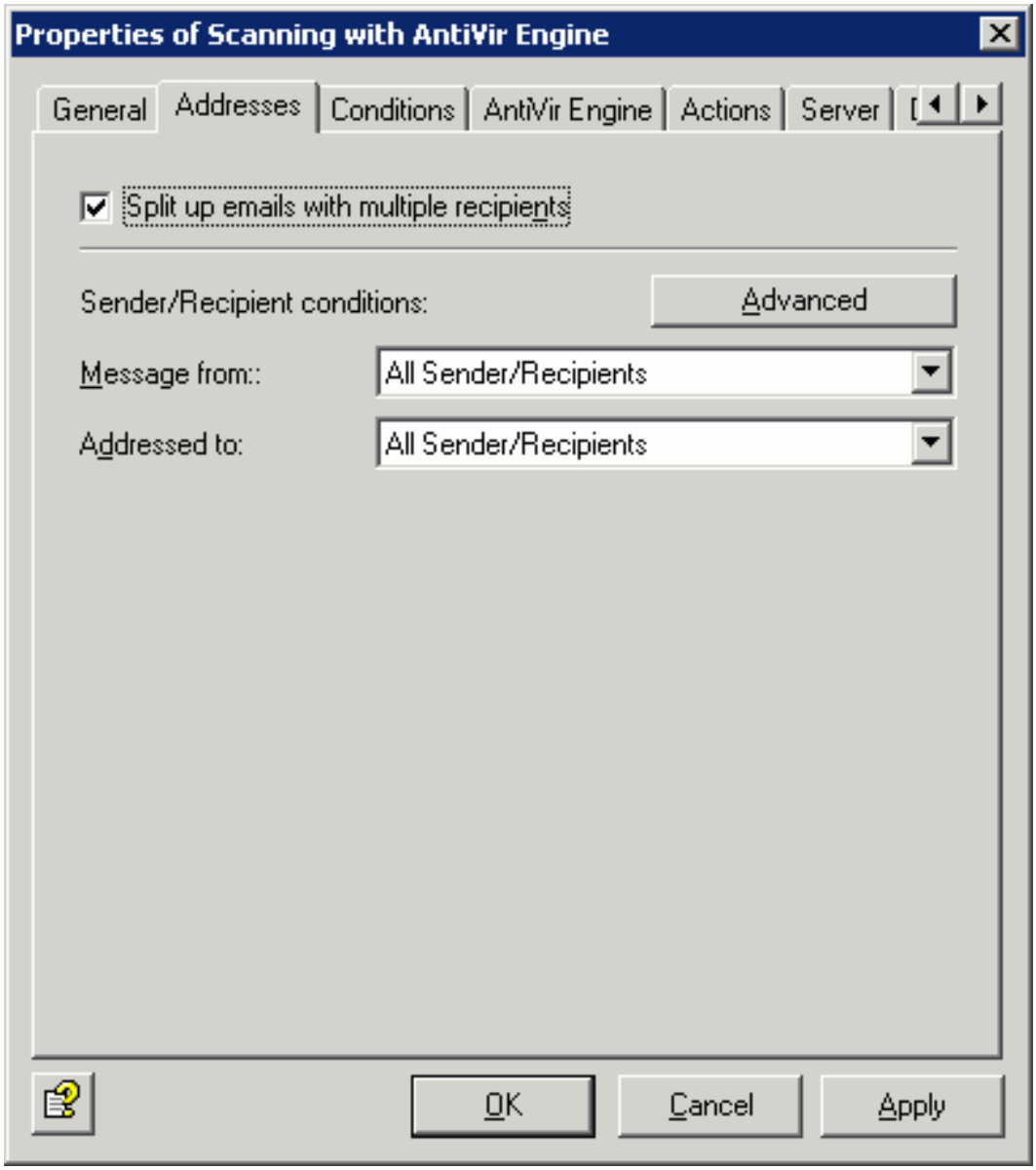
Scanning for viruses

Corporate policy: You want to scan all messages for viruses. In this case it is not enough to scan messages from external domains only: you also have to make sure that no infected mail leaves the company. The specified actions (scanning for viruses, if necessary cleaning the file and sending a copy to Quarantine), must therefore be

performed regardless of the sender and recipient address.

Implementation: The action is executed for **Message from:** <All Senders/Recipients> and **Addressed to:** <All Senders/Recipients>. There are no exceptions. Each mail from each sender to each recipient is checked for viruses.

The following are the address settings for the job:



The **Advanced** window of the **Addresses** tab provides options for an easy implementation of more complex corporate policies . Click on the **Advanced** button, and when finished, click the **Basic** button to return to the standard selection.

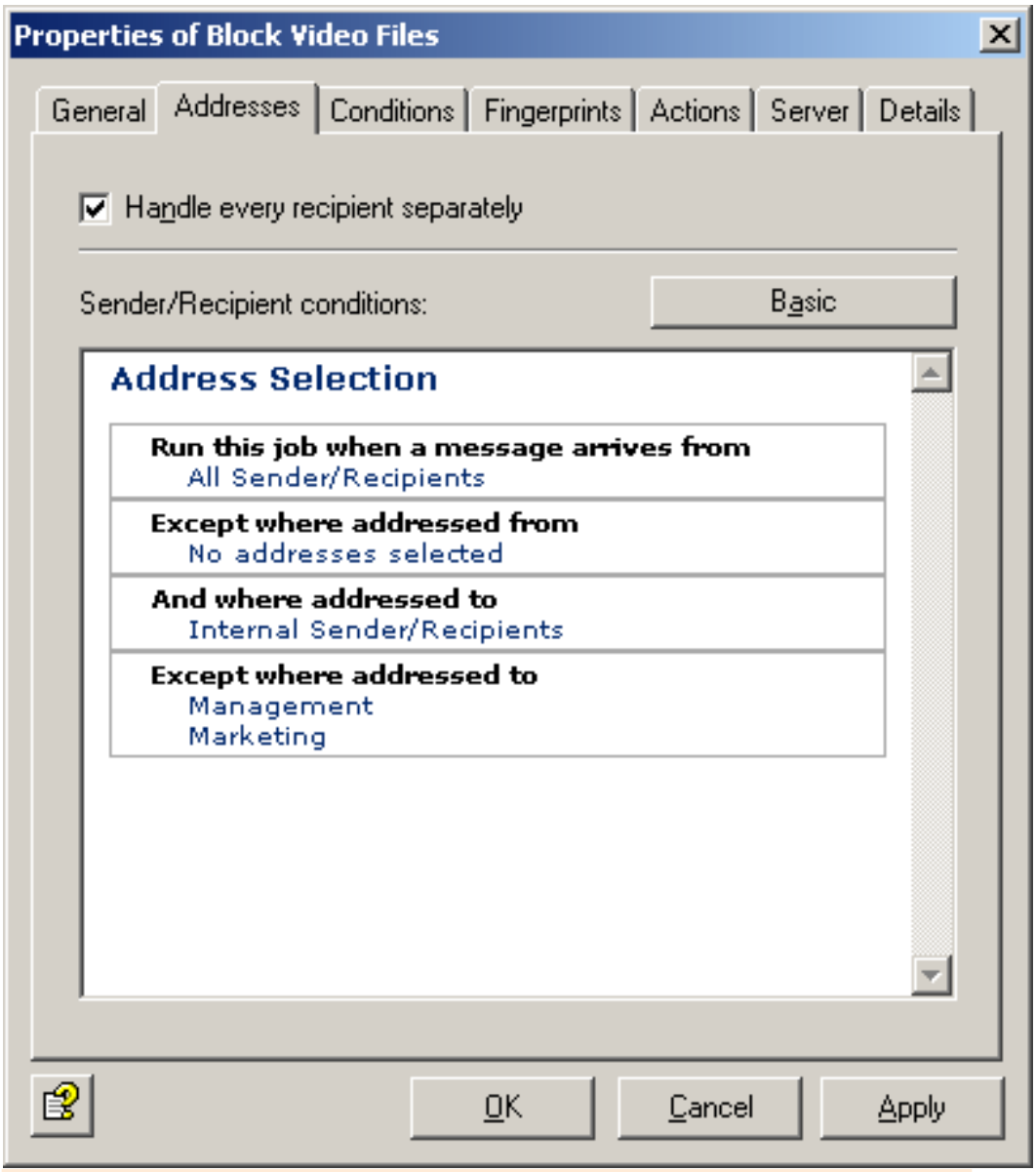
Job for blocking file attachments

Company policy: Let us assume you want to block messages with attached video files from Internet domains unless they are addressed to Marketing or Management.

- **Run this job when a message arrives from** checks the sender(s). So does the exception **Except where addressed from**.

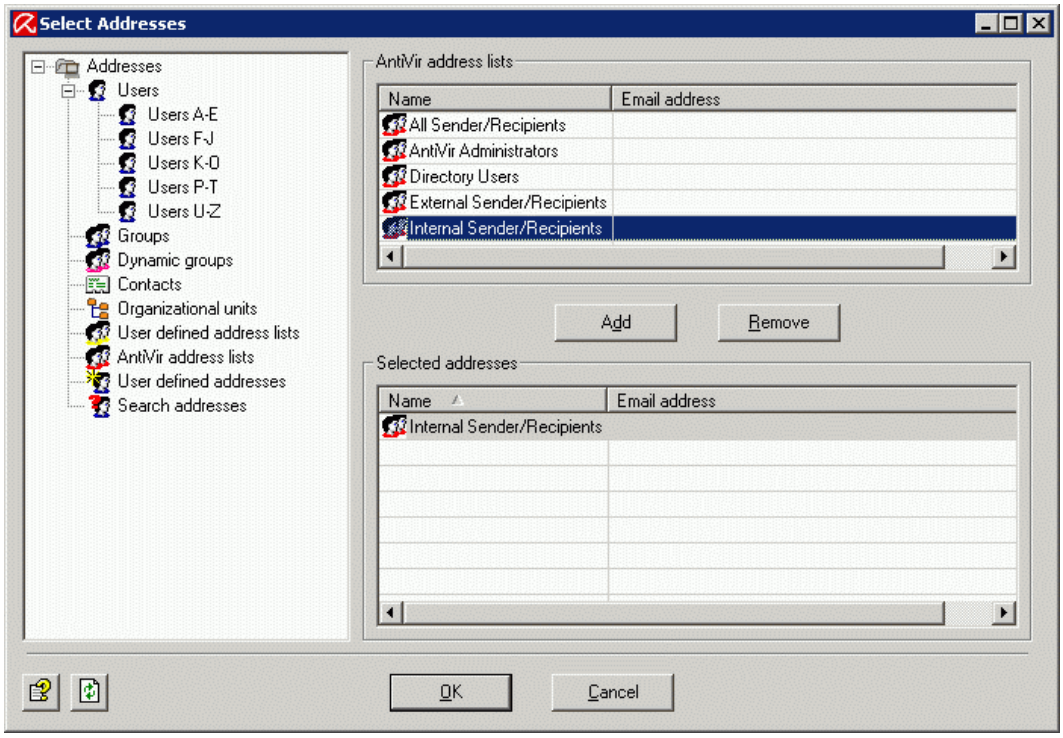
- **And where addressed to** checks the recipient(s). So does the exception **Except where addressed to**.

Implementation: The address settings in the job should look as follows: The specified job action (i.e. blocking files with video attachments) is performed for the `<External Senders/Recipients>` specified under **Run this job when a message arrives from** and is not performed for the `<Internal Senders/Recipients>` specified under **And where addressed to**. Under **Except where addressed to**, enter the Marketing and Management addresses. If you have not already entered these as a group in the Active Directory, you can enter them individually. All video attachments from external senders to internal recipient will now be blocked unless the recipient is a member of the Marketing department or a corporate manager. These are the address settings for the job:

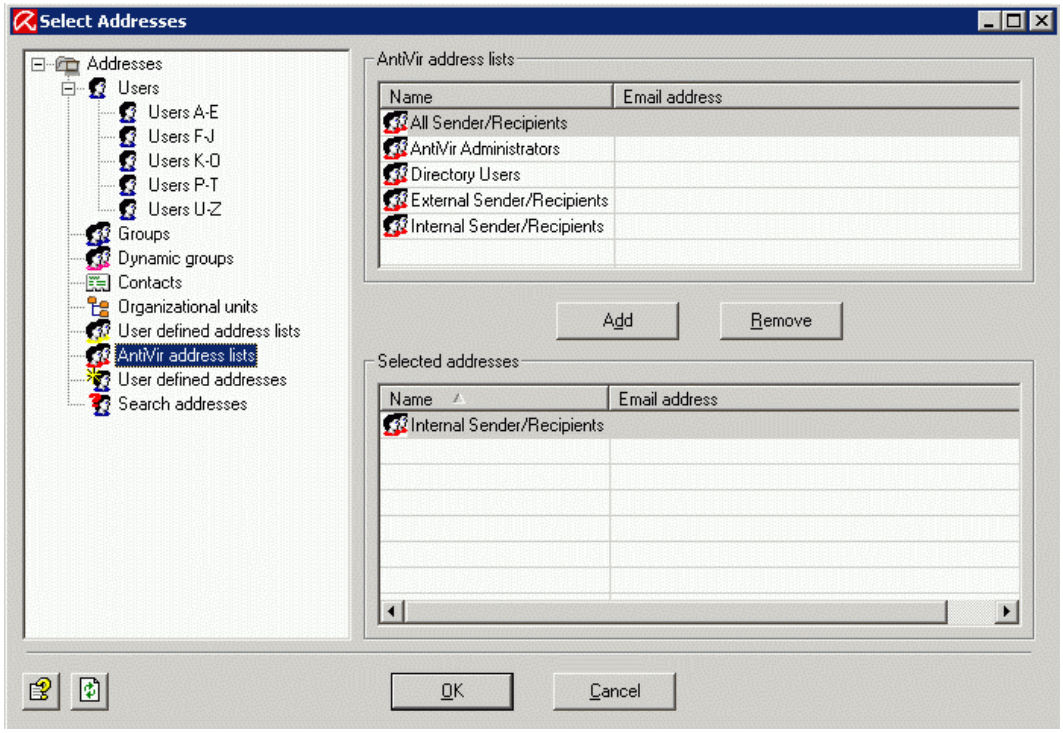


Note: *As a general rule, all of the conditions specified in the **senders** and **recipients** fields must be fulfilled for an action to be initiated (logical AND). If several addresses are entered within the same condition (e.g. **senders**), only one has to apply to trigger the action. The exceptions (**except where addressed from/to** ...) have no effect on the initiation of this action. Messages to or from these addresses are forwarded without performing any of the actions defined.*

To specify the addresses for a specific condition, click **Internal Senders/Recipients**, **No addresses selected** or a corresponding entry in the exceptions. This opens the Select Addresses dialog:



You can also use the **AntiVir address lists**:



The Avira AntiVir Exchange address lists are permanent lists, generated from the global Avira AntiVir Exchange Server settings that are prompted for and entered during

installation or which you have configured manually. Also refer to Avira AntiVir Exchange Server settings .

***Tip: User defined address lists** and **AntiVir address lists** are available only when you select addresses for a job. **User defined address lists** can be edited at any time; **AntiVir address lists** cannot be edited at all.*

3.3.1.6 Creating Notification Templates

In each job, under **Actions**, you can specify the persons to be notified when Avira AntiVir Exchange has intercepted a denied message.

You can create new jobs using templates: simply select the appropriate template for the job type. For further information on the individual job types refer to Policy Configuration .

The notification templates for the individual jobs (content filtering, virus scanning, etc.) are created under **Basic Configuration**.

Creating a notification template

You can find standard notification templates for each module under **Basic Configuration - General Settings - Templates**.

1. Click **Templates** and select the template type.
2. In the right pane, right-click the template you want to use and select **Properties**.
3. Enter the **Notification Subject**.
4. For the notification body text, select the **Notification Body** tab and click **Edit**. To add layout to your text with HTML, use the Formatting toolbar. To enter HTML tags directly, open the source code with the **Source** button.
5. The **Jobs** tab lists the jobs that use the notification template.
6. Click **OK**.

List of Notification Variables

The following variables can be entered in notification texts and notification subject lines. Click on the arrow next to the **Variable** button to insert them directly. Note that the tokens [VAR] and [/VAR] are **case-sensitive** and must always be written in capital letters.

General

Category: variable type	Variable	Description
General: Sender	[VAR]Mailsender[/VAR]	Sender of the message that triggered the action.
General: Sender (SMTP)	[VAR]From[/VAR]	Sender SMTP of the message that triggered the action.
General: Subject	[VAR]Subject[/VAR]	Subject line of the message that triggered the action.
General: Date and Time	[VAR]Date[/VAR]	Date and time at which the job that started the action was run
General: Date	[VAR]DateOnly[/VAR]	Date on which the job that started the action was run
General: Recipient(s)	[VAR]Recipients[/VAR]	Recipients of the message that triggered the action.

Category: variable type	Variable	Description
General: Job Name	[VAR]Jobname[/VAR]	Name of the job that started an action
General: Non-applicable recipients	[VAR]UnrestrictedRecipients [/VAR]	Recipients of the message that triggered the action who were not defined in the (inbound) address conditions.
General: Quarantine folder	[VAR]Quarantine[/VAR]	The Quarantine in which a message was placed.
General: ID of a Quarantine e-mail	[VAR]QuarantineDocRef[/VAR]	Unique identifier of the quarantined mail
General: Server	[VAR]Server[/VAR]	Server through which the affected message was sent; here: the name entered in the configuration settings.
General: Server (network name)	[VAR]ServerFQDN[/VAR]	Server through which the affected message was sent; here: the server's network name (Fully Qualified Domain Name).
General: Time	[VAR]TimeOnly[/VAR]	Time at which the job that started the action was run
General: Avira AntiVir Exchange Report	[VAR]ToolReport[/VAR]	Summary of the scan results
General: Avira AntiVir Exchange Report (Details)	[VAR]ToolReportDetails[/VAR]	Result of the scans with all details
General: Applicable recipients	[VAR]RestrictedRecipients[/VAR]	Recipients of the message that triggered the action who were defined in the (inbound) address conditions

AntiVir

Category: variable type	Variable	Description
AntiVir: Attachment size	[VAR]AttachmentSize[/VAR]	Size of the denied/infected attachment
AntiVir: Attachment type	[VAR]FingerprintName[/VAR]	Name of the denied file type
AntiVir: Fingerprint category	[VAR]Fingerprintcategory[/VAR]	Category of the denied file type
AntiVir: e-mail size	[VAR]MessageSize[/VAR]	Overall size of the message
AntiVir: Attachment name	[VAR]AttachmentName[/VAR]	Names of the denied/infected attachments
AntiVir: E-mail size limit	[VAR]SetSizeLimit[/VAR]	Maximum message size specified in the job
AntiVir: Virus name	[VAR]Virusname[/VAR]	Names of the found viruses
AntiVir: Virus scanner	[VAR]VirusScanner[/VAR]	Names of the scan engines that have found the virus

Information Store Scan

Category: variable type	Variable	Description
IS-Scan: Database	[VAR]VSAPI_Database[/VAR]	Name of the Information Store in which the message was located at the time of the virus scan
IS-Scan: Database URL	[VAR]VSAPI_Url[/VAR]	URL of the Information Store, in which the message was located at the time of the virus scan
IS-Scan: Error description	[VAR]VSAPI_ErrorText[/VAR]	Further description in the event of an error through the Information Store job
IS-Scan: Submit time	[VAR]VSAPI_SubmitTime[/VAR]	Date and time at which message was sent
IS-Scan: Message URL	[VAR]VSAPI_MessageUrl[/VAR]	Information Store URL of the message at the time of the virus scan
IS-Scan: Folder	[VAR]VSAPI_Folder[/VAR]	Name of the Information Store folder in which the message was located at the time of the virus scan
IS-Scan: Mailbox	[VAR]VSAPI_Mailbox[/VAR]	Name of the mailbox in which the message was located at the time of the virus scan
IS-Scan: Server	[VAR]VSAPI_Server[/VAR]	Name of the server on which the virus scan was performed through the Information Store scan
IS-Scan: Virus scanner	[VAR]virusscanner[/VAR]	Names of the scan engine that has found the virus
IS-Scan: Virus name	[VAR]virusname[/VAR]	Names of the found viruses
IS-Scan: Delivery time	[VAR]VSAPI_DeliveryTime[/VAR]	Date and time at which message was delivered

Wall

Category: variable type	Variable	Description
Content filtering	'	'
Wall: Detailed content checking	[VAR]DeniedContentTabHTML [/VAR]	Detailed information on the words/ sentences found
Wall: Mail part	[VAR]DeniedMailParts[/VAR]	Attachments/ message body texts causing the action
Wall: Restricted dictionaries	[VAR]DeniedWordlists[/VAR]	Dictionaries triggering the action because a value/ threshold was reached
Wall: Restricted words	[VAR]DeniedWord[/VAR]	Word triggering the action because value/ threshold was reached
Spam filtering	'	'
Wall: SCL result	[VAR]SCLAnalysis[/VAR]	Return value of the SCL probability level after having

Category: variable type	Variable	Description
		checked the mail for spam
Wall: Spam analysis details	[VAR]SpamReportHTML[/VAR]	Detailed information on each spam criterion
Wall: Spam probability	[VAR]SpamValue[/VAR]	Calculated spam probability value (from 0 to 100). This value is compared with the individually defined threshold values in the advanced spam filtering job.
Wall: Spam level	[VAR]SpamLevel[/VAR]	AntiVir Wall adds a spam level in the form of an asterisk rating in steps of 10 in the header of each scanned message (e.g. X-SPAM-TAG: * indicates a spam probability between 0 and 10, X-SPAM-TAG: *** a probability between 20 and 30). You can define a rule that looks for this string in the Outlook message header and applies actions to message with more than a certain number of asterisks. For further information on creating rules in Outlook, refer to the Outlook help.
Address Filtering	'	'
Wall: Number of recipients	[VAR]NumberRecipient[/VAR]	Number of recipients to which the message is addressed
Wall: Max. number of recipients	[VAR]SetRecipientLimit[/VAR]	The maximum number of recipients defined in the job
Wall: Restricted senders	[VAR]DeniedSender[/VAR]	Name of the sender that started an action
Wall: Restricted recipients	[VAR]DeniedRecipient[/VAR]	Name of the recipient that started an action
X-Block	'	'
Wall: X-Block: image name	[VAR]XblockAttachment[/VAR]	Name of the offensive image. If several images are found, the one with the highest value is specified.
Wall: X-Block: image result	[VAR]XblockResult[/VAR]	Result value of the offensive image. If several images are found, the one with the highest value is specified.

Quarantine summary report

Category: variable type	Variable	Description
Summary: Sender	[VAR]From[/VAR]	Sender of the summary report
Summary: Reply to	[VAR]ReplyTo[/VAR]	Address to which replies to the summary report are to be sent (NotificationReplyTo)

Category: variable type	Variable	Description
Summary: Subject	[VAR]Subject[/VAR]	Subject of the summary report
Summary: Current summary report date	[VAR]Nowdate[/VAR]	Date at which the current summary report was generated
Summary: Last summary report date	[VAR]Lastdate[/VAR]	Date at which the previous summary report was generated
Summary: Current summary report date and time	[VAR]Now[/VAR]	Date and time at which the current summary report was generated
Summary: Last summary report date and time	[VAR]Last[/VAR]	Date and time at which the previous summary report was generated
Summary: Recipients	[VAR]RcptTo[/VAR]	Recipients of the summary report
Summary: Fully qualified domain name	[VAR]FQDN[/VAR]	Full domain name of the server on which the Quarantine for which a notifications to be generated is located
Summary: List of Quarantine e-mails	[VAR]HtmlList[/VAR]	Complete list of all quarantined items for a recipient with HTML formatting (compulsory field in the Quarantine summary report)
Summary: HTTP port	[VAR]HTTPPort[/VAR]	Port of the HTTP server
Summary: HTTP server	[VAR]HTTPServer[/VAR]	HTTP server through which HTTP user requests are sent
Summary: Quarantine	[VAR]Displayname[/VAR]	Name of the Quarantine from where the message list was generated
Summary: Server	[VAR]Server[/VAR]	Short name of the server where the Quarantine is located for which a notification is to be generated
Summary: Current summary report time	[VAR]Nowtime[/VAR]	Time at which the current summary report was generated
Summary: Last summary report time	[VAR]Lasttime[/VAR]	Time at which the previous summary report was generated

Collective notifications

Category: variable type	Variable	Description
Collective notification: Table of contents	[VAR]TOCList[/VAR]i	Numbered HTML list of all notifications (Subject). Each entry in the list has a link to the corresponding entry in the notification list ("NotificationList" variable).
Collective notification: Notification List	[VAR]NotificationList[/VAR]	HTML list of all notifications (Body), separated by dashes.

Whitelist

Category: variable type	Variable	Description
Whitelist: Whitelist entries	[VAR]HtmlList[/VAR]	Complete list of all entries for a recipient with HTML formatting (compulsory field in the whitelist summary report)
Whitelist: Fully qualified domain name	[VAR]FQDN[/VAR]	Full domain name of the server on which the whitelist for which a notifications to be generated is located
Whitelist: HTTP port	[VAR]HTTPPort[/VAR]	Port of the HTTP server
Whitelist: HTTP server	[VAR]HTTPServer[/VAR]	HTTP server through which HTTP user requests are sent
Whitelist: Display name	[VAR]Displayname[/VAR]	Name of the whitelist from which the list of e-mails was generated
Whitelist: Recipients	[VAR]RcptTo[/VAR]	Recipients of the summary report
Whitelist: Reply To	[VAR]ReplyTo[/VAR]	Address to which replies to the whitelist summary report are to be sent (NotificationReplyTo)
Whitelist: Sender	[VAR]From[/VAR]	Sender of the summary report
Whitelist: Server	[VAR]Server[/VAR]	Short name server on which the whitelist for which a notifications to be generated is located
Whitelist: Size	[VAR]CollectedSize[/VAR]	Size of the whole whitelist
Whitelist: Subject	[VAR]Subject[/VAR]	Subject of the summary report
Whitelist: Summary part	[VAR]SummaryPart[/VAR]	In case more than 3.000 new addresses are to be entered in a whitelist, the user receives several whitelist reports. The variable returns the number of the summary report ("1“ for the first 3000 entries, "2" for the next 3000 etc.).
Whitelist: Send whitelist by web	[VAR]link::HTTP_SendWhitelist [/VAR]	Whitelist request and notification occur through HTTP
Whitelist: Send whitelist by mail	[VAR]link::MAIL_SendWhitelist [/VAR]	Whitelist request and notification occur through an e-mail
Whitelist: Clear whitelist by web	[VAR]link::HTTP_ClearWhitelis [/VAR]	Delete the whitelist through HTTP
Whitelist: Clear whitelist by mail	[VAR]link::MAIL_ClearWhitelist [/VAR]	Delete the whitelist through an e-mail

3.3.1.7 Creating a Database Connection to an SQL-Server

Overview

Connection to SQL servers

Database connections are used to connect Avira AntiVir Exchange to external databases. Thus, rather than using the standard local database based on the Microsoft Jet Engine, it

is also possible to use a Microsoft SQL server, which stores Avira AntiVir Exchange data in an SQL database. The supported databases include MS SQL Server 2000 and MS SQL Server 2005; in addition, MS SQL Server 2005 Express can be used with restricted CPU/memory capacity.

When to use SQL servers

A Microsoft SQL server could be used in multi-server environments without server synchronization in order to ensure that each user receives a single central whitelist only for all servers involved.

A Microsoft SQL server could also be used for Quarantine databases.

If *multiple* SQL servers as well as *multiple* Avira AntiVir Exchange servers are installed in a multi-server environments, the servers can be arranged in pairs. This means that a local SQL server is installed on each Avira AntiVir Exchange server and therefore only one database connection needs to be set up.

Note: *Please note that Avira AntiVir Exchange is optimized for being used as a local database based on the MS Jet Engine. Complex server environments require a number of configurations of both Avira AntiVir Exchange and MS SQL Server, which go beyond the scope of this document. Please contact our Support for details.*

Configuration of the Database Connection

The following sections describe the configuration of database connections between Avira AntiVir Exchange and a Microsoft SQL server. Please note that a distinction is made between a central MS SQL server for central user whitelists and a local MS SQL server for the Quarantine.

SQL Server and Avira AntiVir Exchange Server

If SQL Server and Avira AntiVir Exchange Server are installed on the same computer, the following must be met:

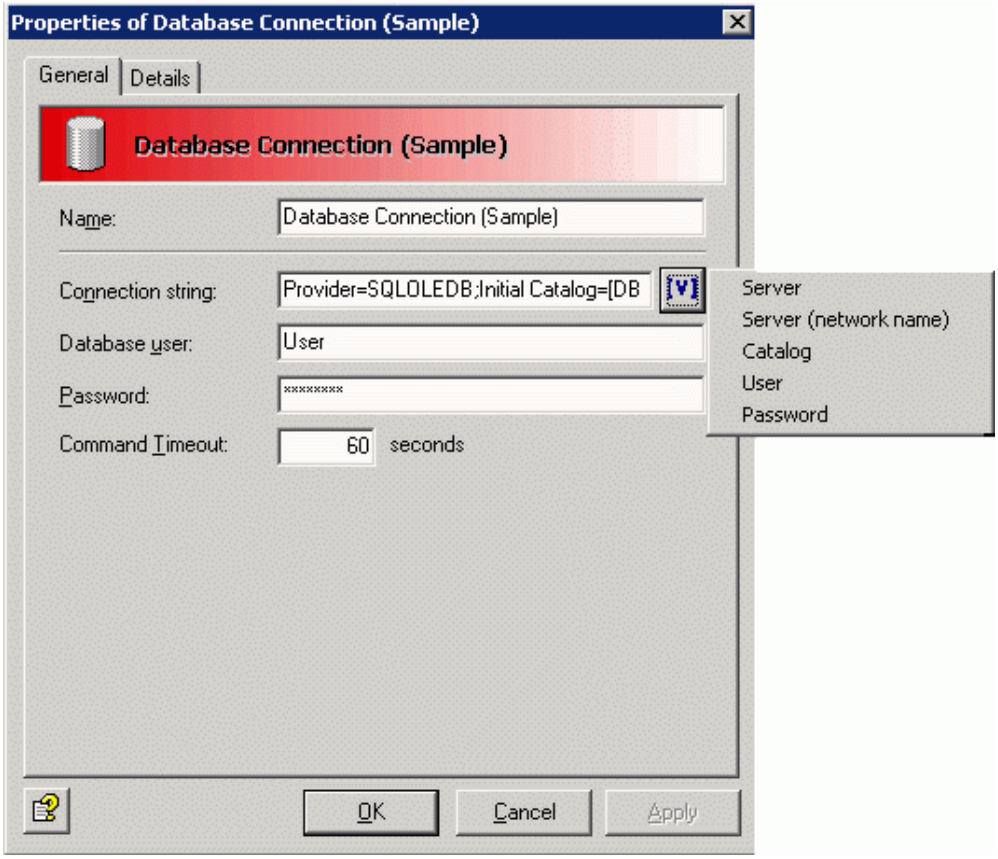
- The installations of SQL Server and Avira AntiVir Exchange Server are complete
- The database(s) have been set up and the corresponding tables created
- At least one user is defined as database user
- This database user has sufficient rights to the database
- The ADO driver has been installed on the Avira AntiVir Exchange server

If SQL Server and Avira AntiVir Exchange Server are installed on different systems, the following has to be additionally ensured:

- The protocol set on the SQL server meets the requirements for external server operation.
- The service has been restarted after completing the SQL Server configuration.

The database connection between Avira AntiVir Exchange and the SQL server is established through the ADO protocol.

1. Under **Basic Configuration - General Settings - Database Connections** create a new database connection.
2. Assign a **Name** for the connection configuration
3. Enter the ADO string information in the **Connection string**field.
4. Enter the required values manually or use the Avira AntiVir Exchange variables available (Server, Catalog, etc.), which will be replaced with appropriate values at runtime.



The **example** below illustrates one of many possible configuration possibilities for the ADO string. For more detailed information on this and other options and configurations of the MS SQL ADO string please refer to the applicable documentation from Microsoft.

Sample connection string:

```
Provider=SQLOLEDB;User
ID=[ADOUser];Password=[ADOPwd];Trusted_Connection=No;Initial
Catalog=[DBCatalog];Data Source=LOCALHOST\SQLEXPRESS;
```

a. `Provider=SQLOLEDB;` mandatory parameter needed to specify the provider. Enter the value manually (no Avira AntiVir Exchange variable available).
b. `User ID=[ADOUser];Password=[ADOPwd];` mandatory parameters; enter the parameters `'User ID='` and `'Password='` manually in the string and set the Avira AntiVir Exchange variables **Database user** and **Password**. The inserted variables `[ADOUser]` and `[ADOPwd]` will be replaced with the contents of the user and password fields below. Using variables is the recommended procedure, as this prevents values in the ADO string from being output in clear text. But it is also possible to enter the values manually, in which case you should leave the user and password fields empty.
c. `Trusted_Connection=No;` optional parameter for SQL authentication. In order for the SQL server to identify the Avira AntiVir Exchange server as Trusted Server, enter `'Trusted_Connection=No;'` manually (no Avira AntiVir Exchange variable available).
d. `Initial Catalog=[DBCatalog];` mandatory parameter, which sets the database to be used. Enter the parameter `'Initial Catalog='` manually in the string and set the Avira AntiVir Exchange variable **Database**. If using the SQL server for the Quarantine, the variable `[DBCatalog]` will be replaced with the name of the database set under **Quarantine - Properties** in

the **Folder name** field. On the other hand, if using the SQL server for a central whitelist, the variable `[DBCatalog]` will be replaced with the fixed name `'Whitelist'`. You can use the `[DBCatalog]` variable to use a database connection for multiple databases within a MS SQL Server. Please note that the databases need to be created exactly under that name. Otherwise any connection attempts will fail!

e. `Data Source=LOCALHOST\SQLEXPRESS;` mandatory parameter for a locally installed MS SQL Server 2005 Express. In this case, enter the `'Data Source='` parameter manually an set the Avira AntiVir Exchange variable **Server** as required. The `[Server]` variable will be replaced with the server's NetBios name at runtime. If working with sub-domains in more complex environments, you can also use the Avira AntiVir Exchange variable **Server (network)**, in which case the `[ServerFQDN]` variable is set and the server's FQDN (Fully Qualified Domain Name) is read. If the SQL server is used for central whitelists, enter the name of the central SQL server manually.

Attention: *Exception: In case of a central SQL server, e.g. to be used for central whitelists, the two Avira AntiVir Exchange variables **Server** and **Server (network)** cannot be used in the ADO string. Enter the name of the SQL server manually, i.e.* `DataSource=Name_of_server;`

5. In the **Database user** field enter the name of the SQL user who is allowed to access the database (shown as User in the figure). In the following field, enter the corresponding **Password**. The values entered here can be retrieved and inserted in the ADO string through the variables `[ADOUser]` and `[ADOPwd]`.
6. Use the **Command timeout** field to set the number of seconds after which the database connection is aborted if no data is returned from the database. For large databases, it is recommended to begin with a value around 60 seconds.

Setting up Central Whitelists

In a multi-server environment, each server creates its own user whitelists. Thus, without server synchronization, each user is provided with a separate whitelist for each of the servers, which all need to be maintained individually. In order to manage these whitelists centrally and simplify administration, you can set up a Microsoft SQL server instead of the standard local database based on the Microsoft Jet Engine. This Microsoft SQL server will write the information for all Avira AntiVir Exchange servers involved to a central SQL database.

To configure central whitelists, a database connection between the SQL server and the Avira AntiVir Exchange server has to be configured first. Then, additional settings are required within Avira AntiVir Exchange in order for Avira AntiVir Exchange to be able to retrieve entries from the whitelist database.

The configuration of the database connection depends on the server environment.

1. Depending on the operating environment, proceed as described in the corresponding scenarios under "Configuration of the Database Connection".
2. Under `Data Source=` enter the central SQL server.

Note: *Please note that in the database connection ADO string, the* `[DBCatalog]` *variable for the whitelist database is replaced with the fixed database name* `'Whitelist'`.

3. Under **Avira AntiVir Exchange Servers - Properties** in the field **Select database connection for whitelist entries** select the SQL server.

   This field provides a selection of all data sources specified under Database connections.

4. Open the Wall job **Advanced spam filtering - Actions - Definite criteria - No Spam** and enable the option **E-mails from User Whitelist entries**.

Setting up a Quarantine Database

Besides using the Microsoft SQL server for whitelists, it can also be used locally for Quarantine databases. Normally, the index of a quarantine is maintained in the local database (Microsoft Jet Engine). In case the capacity of a Jet database is insufficient, these entries can also be written to a locally installed SQL server. This requires having installed MS SQL on the mail server.

The configuration of the database connection depends on the server environment.

1. Depending on the operating environment, proceed as described in the corresponding scenarios under "Configuration of the Database Connection".
2. On each server, set `Data Source=` to `LOCALHOST` in order to access the locally installed SQL server.

Note: *Please note that in the database connection ADO string, the `[DBCatalog]` variable for the Quarantine database is replaced with the folder name under* ***Quarantine - Properties - Folder Name****. This allows to use one database connection for several Quarantine databases.*

When using SQL databases, it could happen that the database service fails or becomes inaccessible. As a result, the Quarantine cannot be accessed during that period of unavailability and any e-mails that should have been quarantined cannot be stored properly. To handle e-mails when the Quarantine is unavailable you can enable the option **Quarantine is mission critical** (similar to the same option for jobs: **Quarantine - Properties - General**).

As soon as a Quarantine is set to ’mission critical’, any Quarantine error is immediately signaled to the job. The job is stopped and the job troubleshooting routine is started. The action performed with the e-mail (ignore job or move to badmail directory) depends on the ’Mission Critical’ setting in the job.

Troubleshooting SQL Servers

Problems that occur during the installation or configuration of an SQL server can have various causes. Therefore, the troubleshooting steps below can only provide basic information as to possible causes:

- Check the port (default: 1433) or adjust it to your server environment.

  Path for *Microsoft SQL Server 2005*: **Configuration Tools - SQL Server Configuration Manager** under **SQL Native Client Configuration - Client Protocols** - double-click **TCP/IP**.

  Path for *Microsoft SQL Server 2005*: **Configuration Tools - SQL Server Configuration Manager - SQL Server 2005 Services - SQL Server Browser** (Status: Running).

- Make sure the SQL Server browser is enabled.

When a central SQL Server has been installed on a different computer than Avira AntiVir Exchange Server, the following requirements must also be met:

- If using *Microsoft SQL Server 2005*, select **Configuration Tools / SQL Server Surface Area Configuration / Surface Area Configuration for Services and Connections**. Under **MSSQLSERVER/Database Engine/Remote Connections** select the option **Using both TCP/IP and named pipes** in order to authorize the connection on the SQL server as configured in the ADO string.

- After configuration is complete, the SQL Server service has to be restarted.

Tip: *Also refer to the Quarantine configuration options (**Quarantine is mission critical**) in case of a database service failure described in the preceding section.*

3.3.1.8 Folder Settings

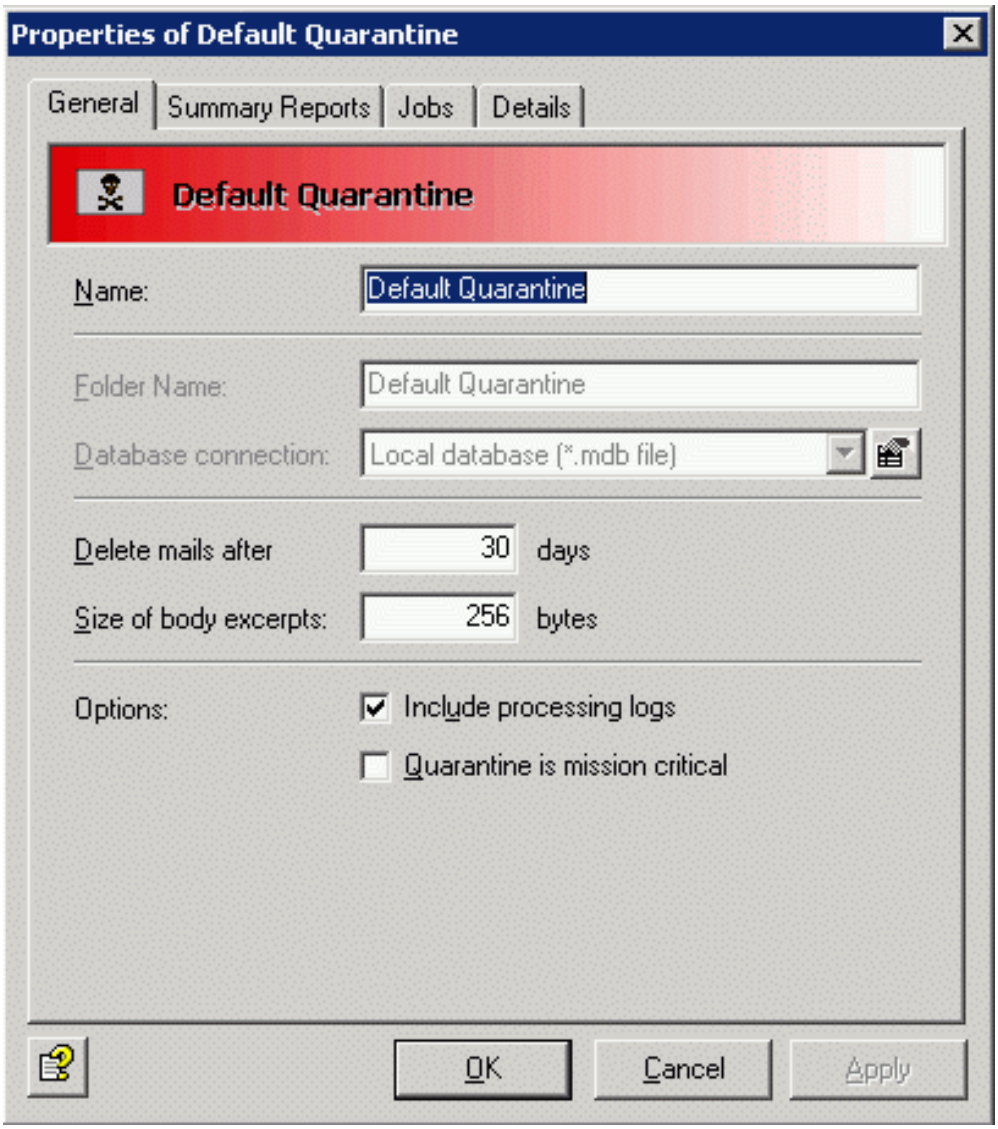
Quarantines Configuration

A Quarantine is a directory in which all messages are placed that meet the criteria defined for the **Copy to Quarantine** action. When Avira AntiVir Exchange is installed, a folder named `Quarantine` is created in the data directory, which initially contains a few default quarantines and later all other new quarantines.

1. Select **Basic Configuration - Folder Settings - Quarantines** to configure the existing quarantines and set up new ones.

   In the right window section, all available quarantines are shown.

2. Right-click an existing Quarantine in the right pane and select **Properties**.



3. Under **Name**, enter a descriptive name for the Quarantine.

   The Quarantine's **Folder Name** remains the same. This option is only available when you create a new Quarantine.

4. Set after how many days a quarantined mail is to be automatically **deleted**.
5. Use the **Size of body excerpts** field to set whether or not and how much text from the body of the mail (message text) is to be stored in the database.

   When setting this field, please take into account the privacy aspects and the required space in the database.

Note: *The size of a Quarantine is limited to 1 GB!*

6. The **Include processing logs** field can be used to log the processing of quarantined e-mails, e.g. to trace back the reasons for quarantining a mail.

   You can call the corresponding e-mail in the AntiVir Monitor and view the **Processing Log** including all details.

7. **Quarantine is mission critical**:

   If enabled, any Quarantine errors are signaled to the job, after which the job is stopped and the job troubleshooting routine is started. The action performed with the e-mail (ignore job or move to `badmail` directory) depends on the 'Mission Critical' setting in the job. For additional information on the mission-critical jobs refer to This job is mission-critical .

   Example: An anti-virus job detects a virus in an incoming e-mail. According to the job configuration, the e-mail is to be moved to the default Quarantine and not to be delivered to the recipient. Due to a Quarantine error however, the e-mail cannot be quarantined.The following settings for the job and the Quarantine are conceivable:

   a. Both Quarantine and job are NOT mission-critical:

      The Quarantine error will be ignored. The mail cannot be quarantined, but it is not delivered either.

   b. The Quarantine is NOT mission-critical + the job IS mission-critical:

      Result: the same as above.

   c. The Quarantine IS mission-critical + the job is NOT mission-critical:

      The job is aborted and the infected(!) mail is passed as it is, to the next job in the processing chain.

   d. Both Quarantine and job ARE mission-critical:

      The mail is moved to the `BADMAIL` Quarantine and not delivered.

Attention: *As long as the Quarantine error has not been eliminated, it will systematically be signaled to the job if the 'Mission Critical' option is enabled (for the Quarantine).*

   If the job itself is not mission-critical, it will disable itself after a certain time and no longer process any mails.

   On the other hand, if the job is mission-critical as well, each mail will be moved to the bad mail area (and not delivered) until the error has been resolved!

Regardless of the actual 'mission critical' setting, the Avira AntiVir Exchange administrators are informed by e-mail of recurring Quarantine or job errors.

8. Under the **Summary Reports** tab, you can now configure a summary notification for the selected Quarantine.

Note: *In case you allow the users to access and modify whitelists, press* ***Add*** *and select* ***Quarantine Summary Report with Whitelist Support*** *under* ***Template****.*

1. Right-click **Quarantines** and select **New - Quarantine**.
2. The **Folder Name** is taken from the description. Only the characters A - Z and 0 - 9 are used, all others are converted into underscores.
3. The proposed **Folder Name** can be overwritten.

Note: *Enter the folder name only, not an absolute path!*

4. When you have saved the configuration, these quarantines are automatically created by the EMH and displayed in the Avira AntiVir Exchange Monitor (after you press Refresh).

Note: *The size of a Quarantine is limited to 1 GB!*

Defining Quarantine Summary Reports

Quarantine Summary Reports provide information on the messages quarantined by Avira AntiVir Exchange, the Whitelist Summary Reports on the new entries in the user whitelist.

Summary reports can be sent to various recipients or recipient groups and contain a list of various quarantined messages. The listed messages, the actions the user can take when receiving a summary report and the additional information contained therein are defined separately for each summary report.

Summary reports consist of two parts:

- The template, which contains variables and defines the form of the notification.

  To edit the summary report template, select **Basic Configuration - General Settings - Templates - Quarantine Summaries**. The variables used here apply only to the summary report and its form. Configure the summary report template as described under Creating Notification Templates .

- The list of quarantined e-mails (the actual content of the summary notification).

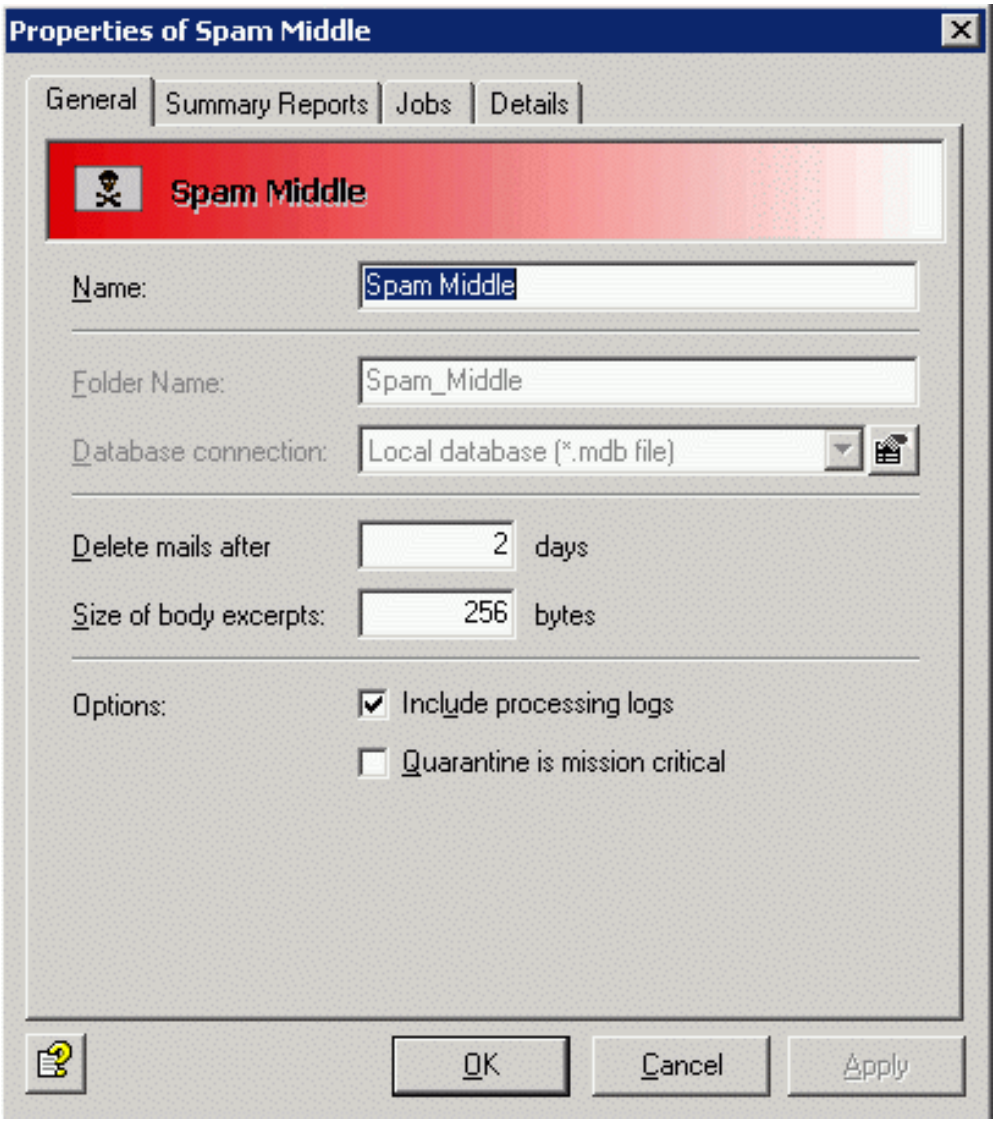
  Fields are used to define which e-mails and which e-mail fields are to be listed in the summary notification.

  The content of the summary report, i.e. the list of quarantined messages, is set by the **Summary: Quarantine e-mail list** (`[VAR]HTMLList[/VAR]`) variable, which must be set for every summary report. The entries recorded in the list are specified under **Folders - Quarantines - Properties - Summary Reports - Add - Summary fields**.

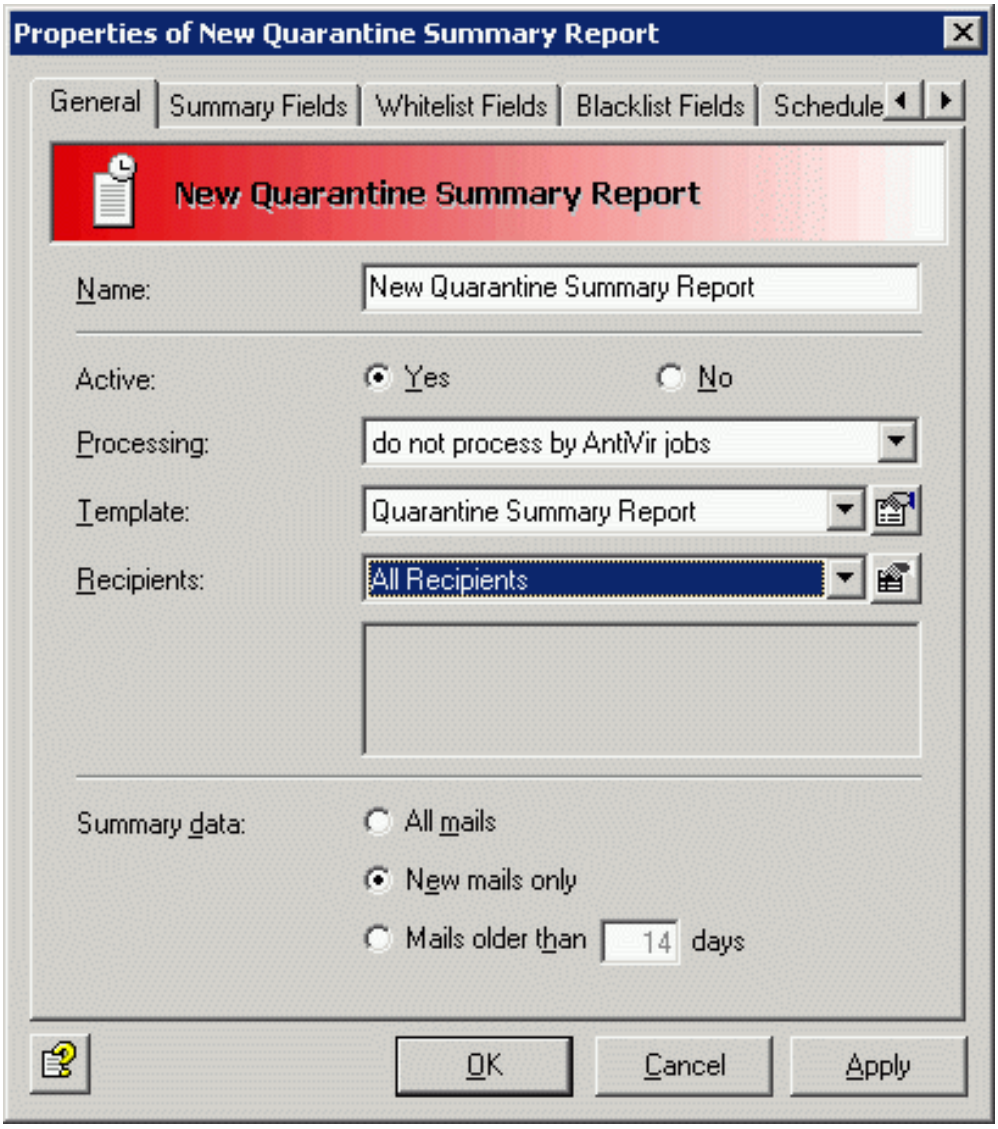
The variable **Summary: Sender** under **Templates** refers to the sender of the summary report (the same sender as for all Avira AntiVir Exchange notifications; to be defined under **AntiVir Servers Settings**). The **Sender** checkbox in the **Fields** tab for a Quarantine specifies that the sender of the quarantined message will be shown in the list.

Summary reports are especially useful for spam quarantines and the recipients of spam. Users will normally receive a list of all new spam messages that were addressed to them and have been placed in a particular Spam Quarantine. Set up reporting for this scenario as follows:

1. Open **Basic Configuration - Folders - Quarantines**.
2. In the right window section, double-click the spam Quarantine **Spam: Middle** to open it.



3. Select the **Summary Reports** tab.
4. Click **Add**.
5. Select the **General** tab and enter a **Name** for the summary report.



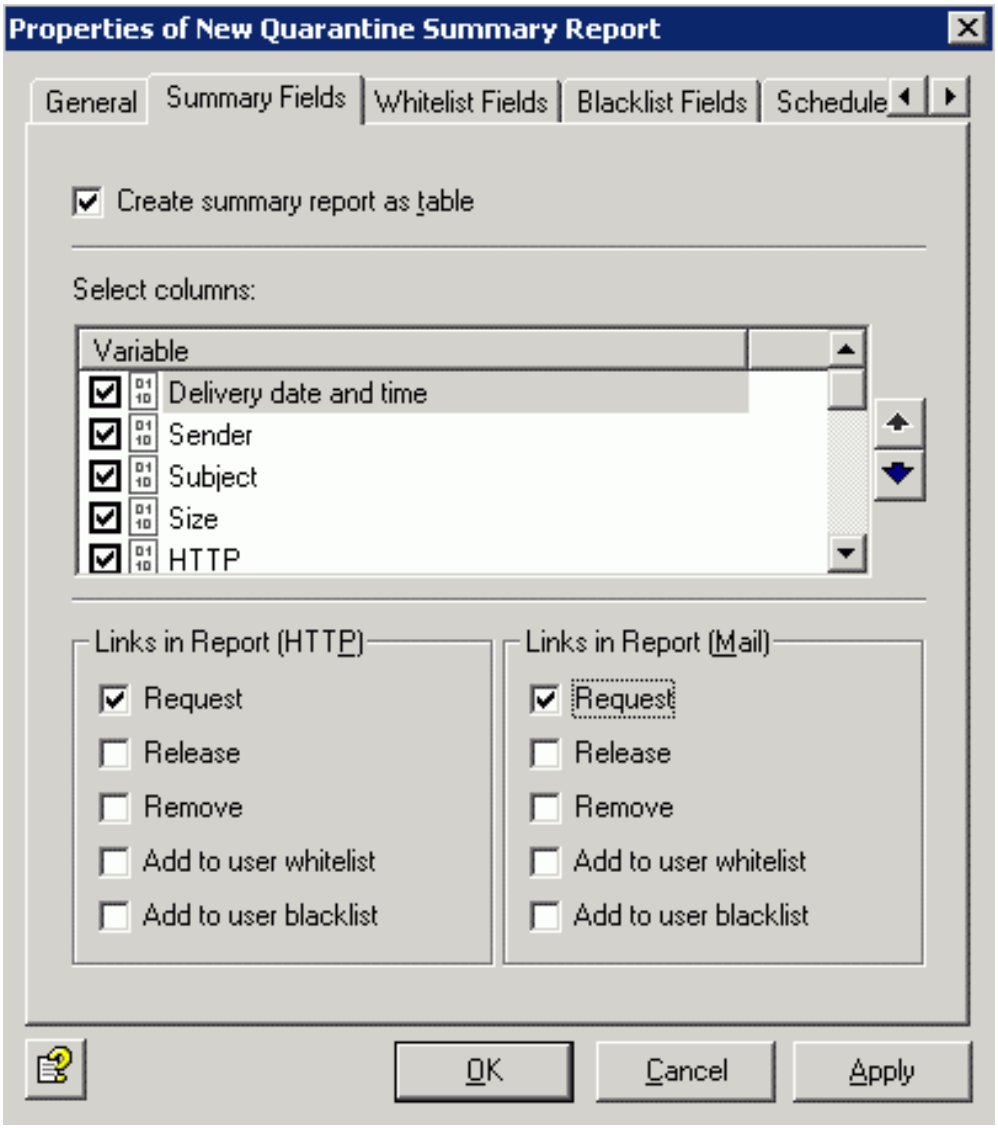
6. In the **Recipients** field, select **All Recipients**. The original recipients of the quarantined messages will receive the summary report. Select **Userdefined Recipients** when you want to limit the group of recipients of a summary report. The selected recipients, senders, groups or other address patterns are listed in the text field under the **Recipients** field.

7. As **Template** you can use a summary report that you have created yourself under **General Settings - Templates - Quarantine Summary Report**. By default, Avira AntiVir Exchange contains the preconfigured **Quarantine summary report** template. If you wish to allow the users to add a sender to their user whitelist from within the summary notification, use the template named **Quarantine Summary Report with Whitelist Support**.

8. For the **Summary data** (report's contents) select **New mails only**. The summary report will then list only those messages that have been quarantined since the last summary report.

9. **Processing: do not process by AntiVir jobs** means that messages resent or released on the user's request are not checked by enabled AntiVir jobs, but are delivered to the recipient without further processing. Also refer to the next tab, **Summary Fields**.

10. In the **Fields** tab, select the message fields to be listed in the quarantined messages summary report. If, for example, you check **Subject** here, the subject of the quarantined messages is listed in the summary report. A default selection is already preselected.



Users can click the links in the summary report to perform actions with the selected messages. Select the actions the user will be allowed to perform:

Request: The quarantined message is forwarded to the recipient of the summary report.

Release: The message is forwarded to all original recipients.

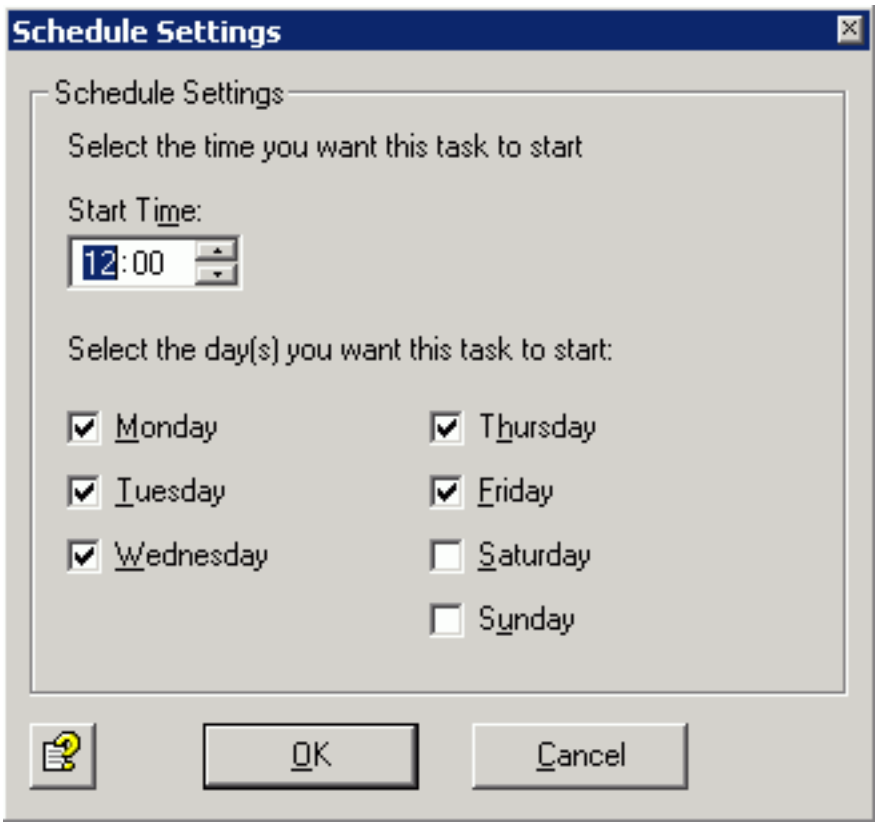
Remove: The quarantined message is marked for deletion.

Add to user whitelist/ blacklist: The sender of the e-mail is entered in the user's whitelist/ blacklist.

Note: *Each of the options you select in the* ***Fields*** *tab will appear as a separate link in the summary report.*

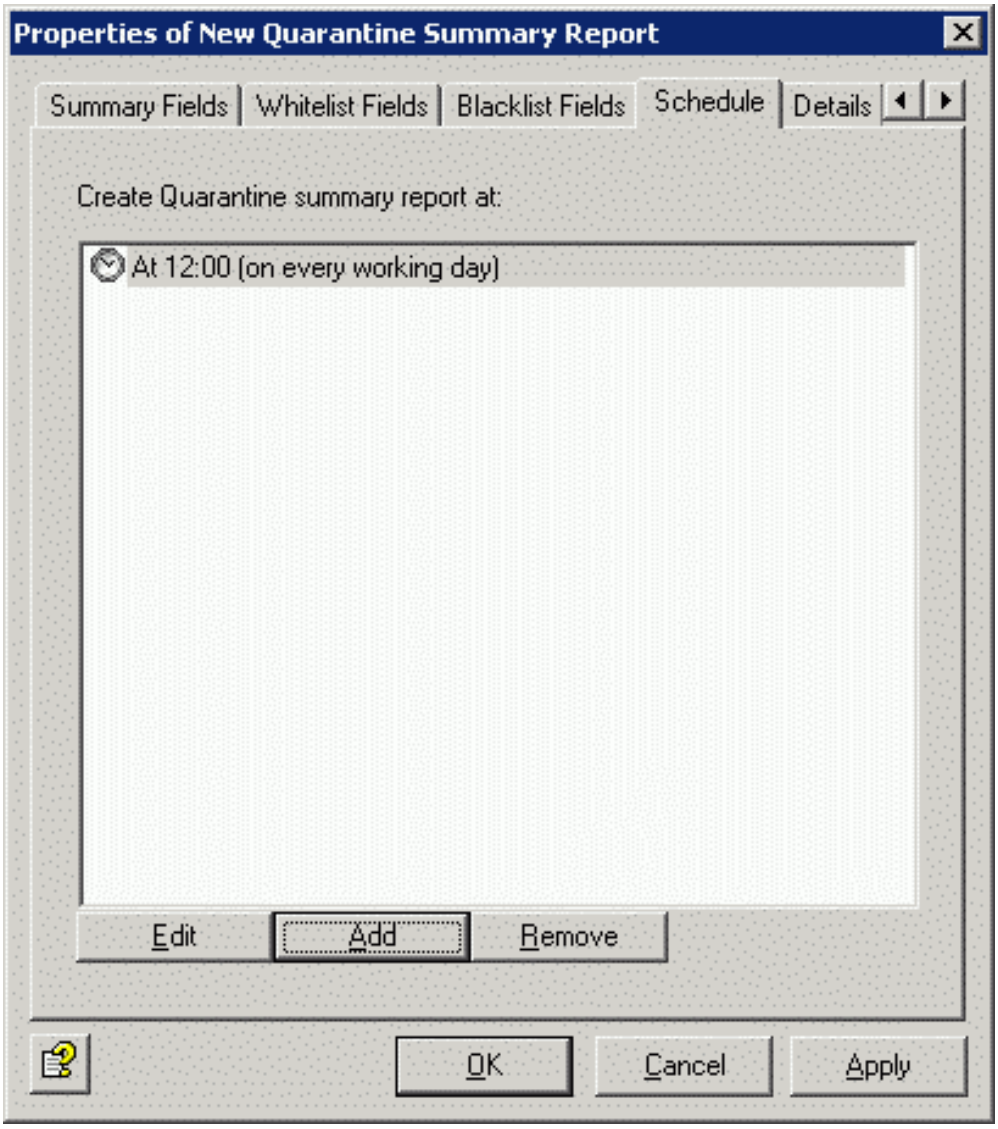
11. In the **Whitelist Fields** tab select the message fields to be listed in the whitelist notification.

12. Select the **Schedule** tab and click **Add**. A Schedule Settings dialog opens in which you can specify the time at which summary reports will be generated. In the example below, a summary report is sent to the recipient of the spam mail daily at 12 o'clock (12:00 AM hours).



13. Click **OK**.

14. The new Quarantine summary report now appears in the **Schedule** tab. To change the time or day, click **Edit**; to delete the summary, click **Remove**.

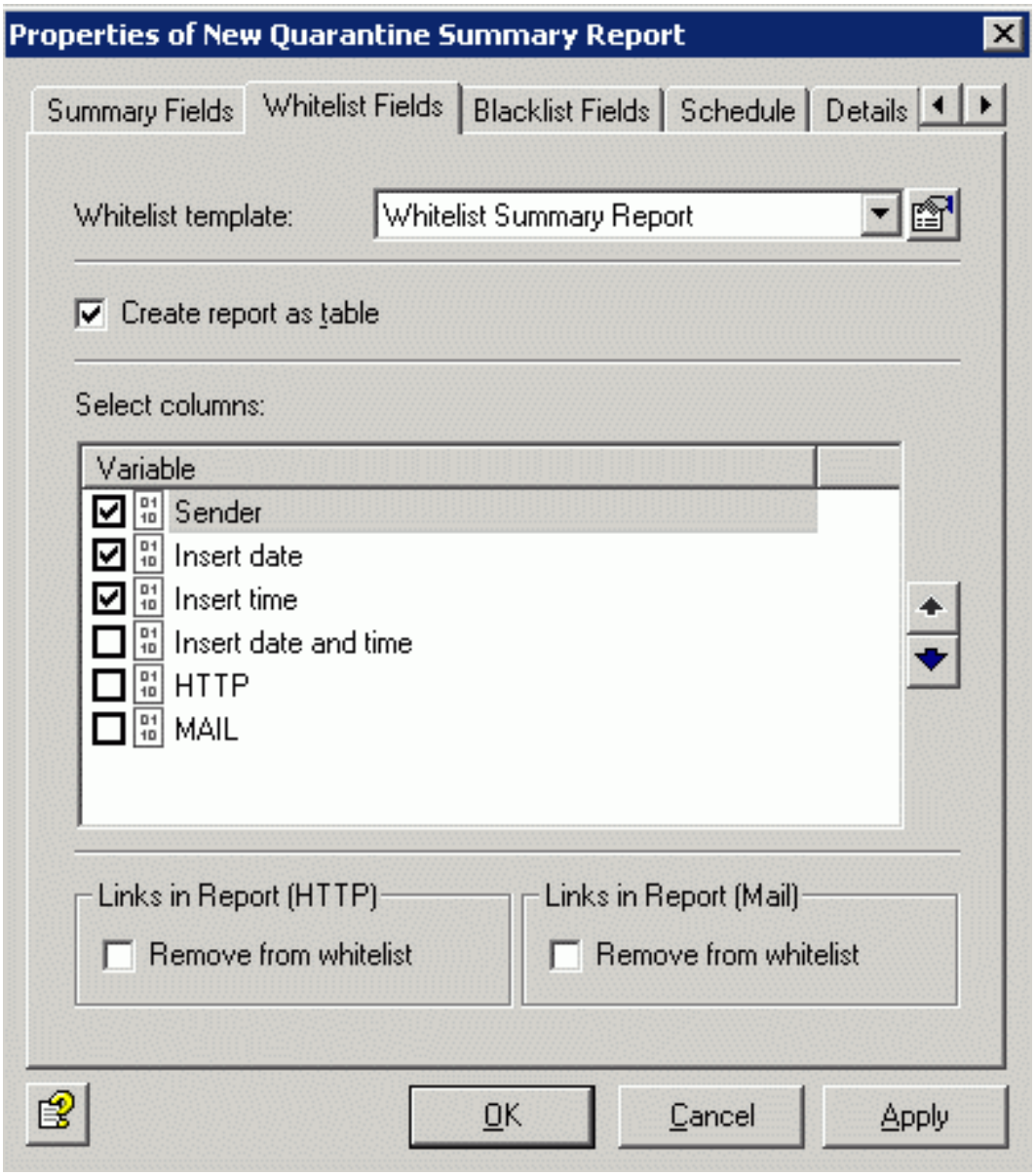


Summary reports will be sent at 12:00 AM to the recipients of spam mail quarantined in **Spam Middle**.

Note: *You can create several different summary reports with differing contents for a single Quarantine. For each report, the messages are compiled separately from the Quarantine, even if the reports are scheduled for the same time.*
Tip: *A list of all quarantines is available under* ***Folders - Quarantines****. The* ***Summary*** *column shows the quarantines for which a summary notification has been configured (Yes/No).*

Whitelist Summary Reports

Quarantine Summary Reports also provide information on the messages quarantined by AntiVir in the Whitelist Summary Reports.



For the Quarantine Summary Report, select the template **with Whitelist Support**, so that the recipient of the Quarantine summary report can manage the entries in his whitelist and request a whitelist summary report.

Select the message fields to be listed in the Whitelist Summary Report.

Use the **Whitelist template** field to edit any existing whitelist template or create a new one. Configure the Whitelist template with the variables as described under List of Notification Variables .

3.3.1.9 Utility Settings

Fingerprints

Fingerprints are used by AntiVir to identify file types. A comprehensive range of fingerprints, subdivided into categories, is included with Avira AntiVir Exchange. Normally, you do not have to make any changes to these fingerprints. Refer to Configuring Fingerprints .

Dictionaries

Here, you can create dictionaries of text strings that you want AntiVir Wall content and spam filtering to block. We have already created a few dictionary categories that you can customize to your requirements. Refer to Setting up Dictionaries .

AntiVir Engine

For details on the configuration of the virus scanner, refer to Configuring and Enabling the AntiVir Scanner .

3.3.2 Policy Configuration

The Policy Configuration is used to implement the company policies by way of jobs.

Under Policy Configuration, define your Avira AntiVir Exchange jobs based on your company's own policies.

Using a range of conditions (or filters), you can specify the messages that will be intercepted, the actions to be performed and scheduled, and the priority of each job (i.e. the order in which jobs are run). All conditions can be configured within the jobs. Together, the Avira AntiVir Exchange jobs form your company's policy.

3.3.2.1 Corporate Policy Example

All incoming spam messages are to be detected, deleted and quarantined.

You do not want the junk mail to be delivered, but its recipients should be notified about received spam so that they can decide for themselves which messages to accept.

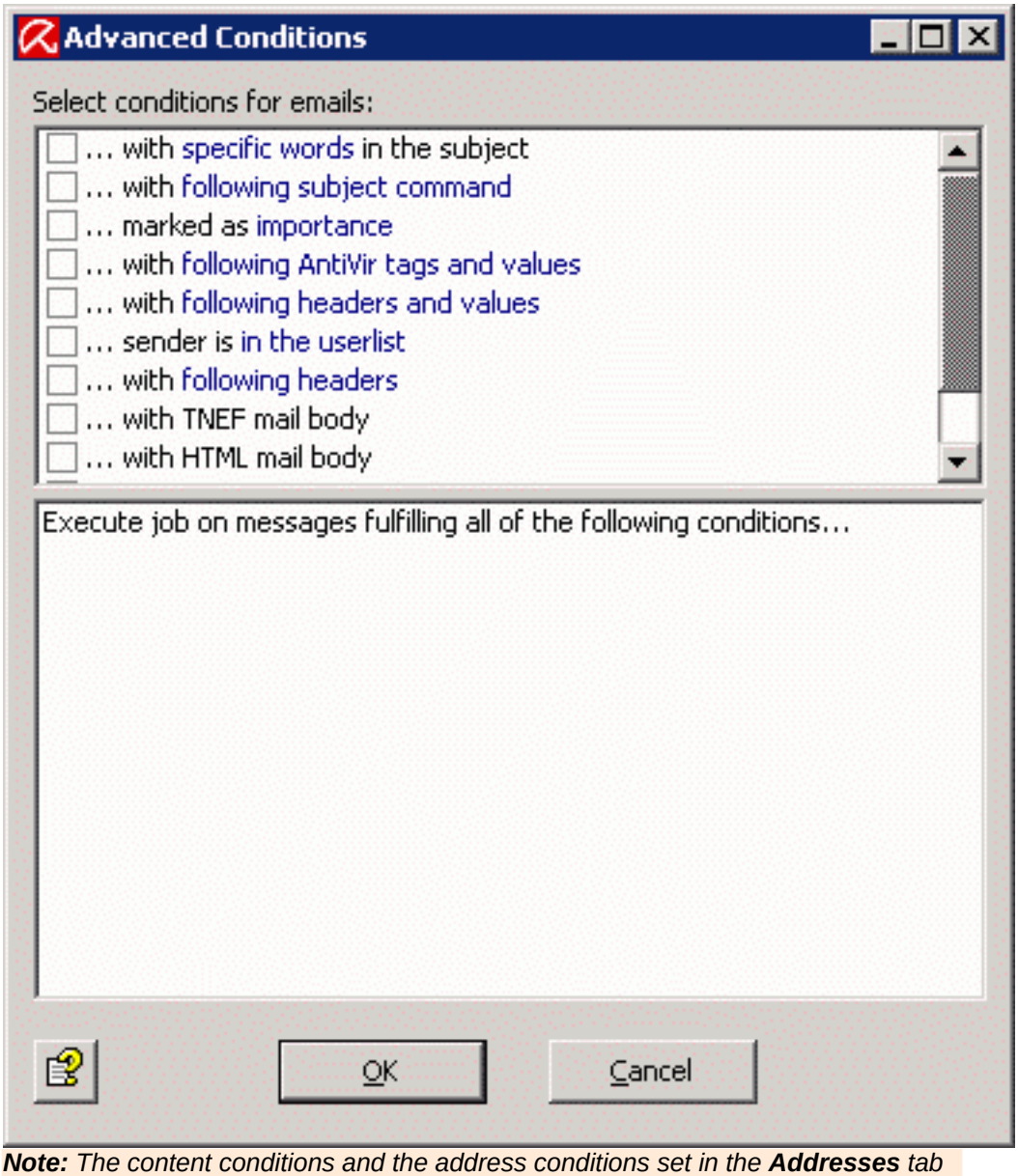
Notifications are to be sent daily in the form of a summary report.

To implement this, use the Wall job **Advanced spam filtering**.

3.3.2.2 Conditions

In each job you can use **Conditions** to set the requirements as to which mails or documents a job is to be run for. To this end, several types of rules are defined by default. You can set the different parameters for a specific condition according to your requirements.

Before a job is run, the rules for this job are evaluated. When **all** set conditions apply, the e-mails or documents are handled by the job. Rules allow the grabber to carry out job requests depending on the information in the individual documents. This enables a very precise selection of documents to be checked.


Advanced Conditions
Select conditions for emails:
... with specific words in the subject
... with following subject command
... marked as importance
... with following AntiVir tags and values
... with following headers and values
... sender is in the userlist
... with following headers
... with TNEF mail body
... with HTML mail body
Execute job on messages fulfilling all of the following conditions...
OK
Cancel

Note: *The content conditions and the address conditions set in the* ***Addresses*** *tab must simultaneously come true, for a job to be run (logical AND).*

The value of X-headers allows to control e-mail processing so that, for instance, the results can be evaluated by open source tools. Moreover, with the condition **...with following headers and values**, it is possible to select all e-mails that do not include headers or do not have the defined value. However, if such control elements must not appear in the header of e-mails, you can use the condition **...with following AntiVir tags and values** instead, as they are not displayed in the message body.

3.3.2.3 Job Types

There are 9 job types, which you can find under **Policy Configuration - Mail Transport Jobs - New**:

Job Type	Function
AntiVir Scanning	Scans messages for viruses.

Job Type	Function
AntiVir E-Mail Size Filtering	Checks messages for size and denies files that are larger than the allowed maximum size (per message size).
AntiVir Attachment Filtering	Checks messages for denied file attachments The various file formats are identified with fingerprints.
AntiVir Attachment/Size Filtering	Checks messages for denied file attachments and for file size, and denies files larger than the specified size.
AntiVir Wall Content Filtering	Checks messages and attachments for restricted text content.
AntiVir Wall Email Address Filtering	Checks messages for address restrictions.
AntiVir Wall Recipient Limit Filtering	Checks messages for a maximum allowable number of recipients per message (the recipients in the To field of each message).
AntiVir Wall Xblock Image Filtering	Checks messages for offensive images.
AntiVir Wall Spam Filtering	Checks messages for spam using a range of criteria.

For each job type, you can define individual conditions, **all** of which must apply for the specified action to be executed. Address filtering can be performed by all job types. You can, for example, create a job that quarantines and deletes all messages (without forwarding them to their recipient) that were sent from the domains *@gmx.net and *@hotmail.com, are larger than 500 KB, contain the word "Look" in the subject field and belong to the fingerprint category **Sound**. This would be an **AntiVir Attachment/Size Filtering Job**.

Avira AntiVir Exchange is delivered with a number of standard jobs, which can be adapted to your requirements. Of course, you can also create your own jobs. Preconfigured jobs are available under **Policy Configuration - Job Templates**. With the mouse, drag the desired job to **Mail Transport Jobs**. There is no limit to the number of jobs you can create. The order in which the jobs will be processed is shown in the job list in **Mail Transport Jobs**. For additional information refer to Job Processing Sequence .

A job can be enabled or disabled. To prevent a job being run, you can simply disable it: you do not have to permanently delete it from your configuration.

For each job, on the **Actions** tab, you can specify the actions to be executed when a message meets the defined criteria or is virus-infected.

3.3.2.4 Actions

In addition to the job-specific actions, you can use the following standard **actions**.

Copy to Quarantine	A copy of the message is placed in the specified Quarantine folder, where it can be viewed any time.
Delete e-mail	The infected/denied message is permanently deleted from the server. If selected, a copy is first placed in Quarantine.
Delete attachment	The infected attachments are permanently deleted

	from the server.
Add a subject extension	A configurable supplement is added to the Subject line to indicate that the message has been processed.
Send notifications to	Notifications can be sent to the following groups and individuals: • Administrators • Sender • Recipients • Other persons
Run external Program	Runs an external program.
Add X-header field	A field is added to the message header, which can be filled with a value from one of the variables.
Redirect mail	The e-mail is resent to the recipients specified. Optionally, the message can also be sent to the original recipients.

3.3.2.5 Job Processing Sequence

The order in which jobs are processed is shown in the job list under **Policy Configuration - Mail Transport Jobs**.

New jobs are added at the end of the list and can be moved to the desired position with the and icons in the icon bar or through the context menu (**All Tasks - Move up/Move down**).

3.3.3 AntiVir Monitor

The AntiVir Monitor allows you to view the Quarantine areas on each available server as well as detailed information on the mails quarantined there.

The AntiVir Monitor is used to observe all **Avira AntiVir Exchange servers**, **quarantines** and **badmail folders**. In addition, it provides access to **statistical evaluations**.

The Monitor lists all servers configured under **Basic Configuration - AntiVir Server**. The AntiVir Monitor accesses the servers via the network using SOAP/SSL encryption.

To enable access to a server, first enter the server under **Basic Configuration - AntiVir Server** and then refresh the **AntiVir Monitor** view.

For details on how to add a server, please refer to Settings for an Individual Avira AntiVir Exchange Server . Also make sure your Quarantine has been set up according to the instructions under Quarantine Configuration .

You can view detailed information on the Avira AntiVir Exchange version, configuration, etc. for each server: in **AntiVir Monitor**, right-click the desired server and select **Properties**.

The AntiVir Monitor requires a logon as authorized user. If you are not logged on to the server locally, a logon dialog will prompt you for a user name and password to access the corresponding domain. The AntiVir Monitor access rights are set in the properties of the

`access.acl` file in the folder `...\Avira\Avira AntiVir Exchange\AppData\`

Select the **Security** tab and provide the desired users at least with write access.

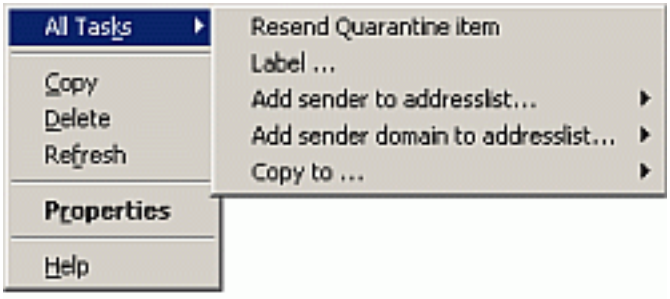
To observe data in the Monitor:

1. Click on the desired server.
2. Authenticate yourself with a user name and a password with sufficient rights to access the Avira AntiVir Exchange data on the server's file system.
3. Click the area you wish to view, e.g. **Default Quarantine** or **BADMAIL**. All available mails will be displayed (up to a maximum of 10.000).
4. Filter the mails using the **Filter Options** icon .
5. Double-click on a mail to open it.
6. Resend mails using the **Resend item**icon as required.

3.3.3.1 Quarantines

If you have enabled the **Copy infected email to Quarantine** action in a job, all affected messages are copied to a Quarantine and the AntiVir Monitor displays all information available on each e-mail.

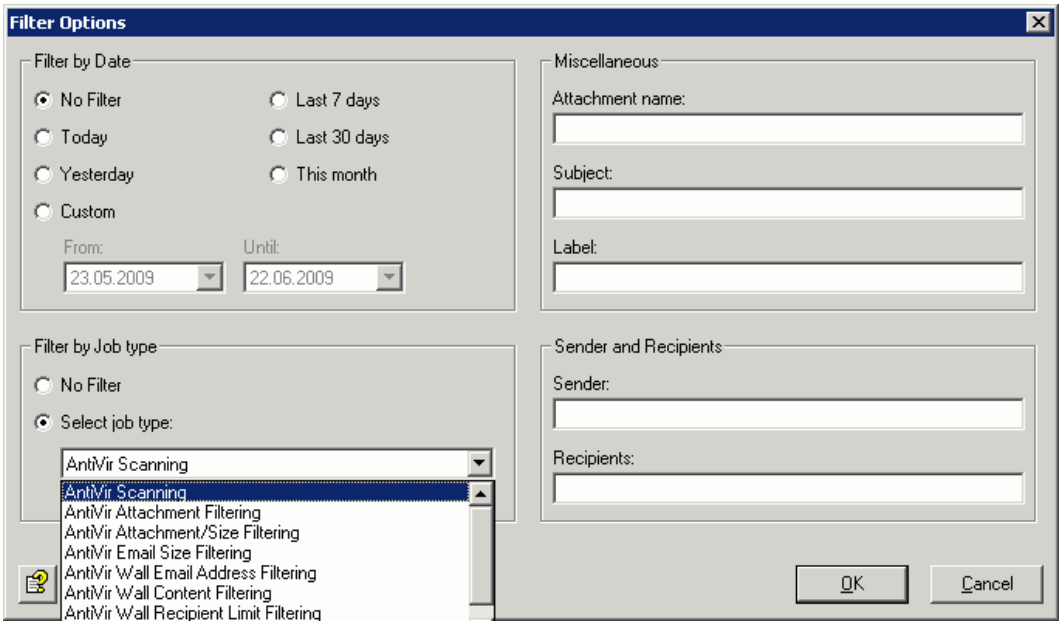
Click on a Quarantine to view a list of mails. If you right-click on a mail, the following options are available:



Copying mails is also possible via drag & drop. With the mouse, simply drag the selected mail to another Quarantine.

Within a Quarantine, you can filter messages according to numerous selection criteria. To do so, right-click **View - Filter options** or click on the icon. The following dialog

appears:



You can reset the options in one of three ways:

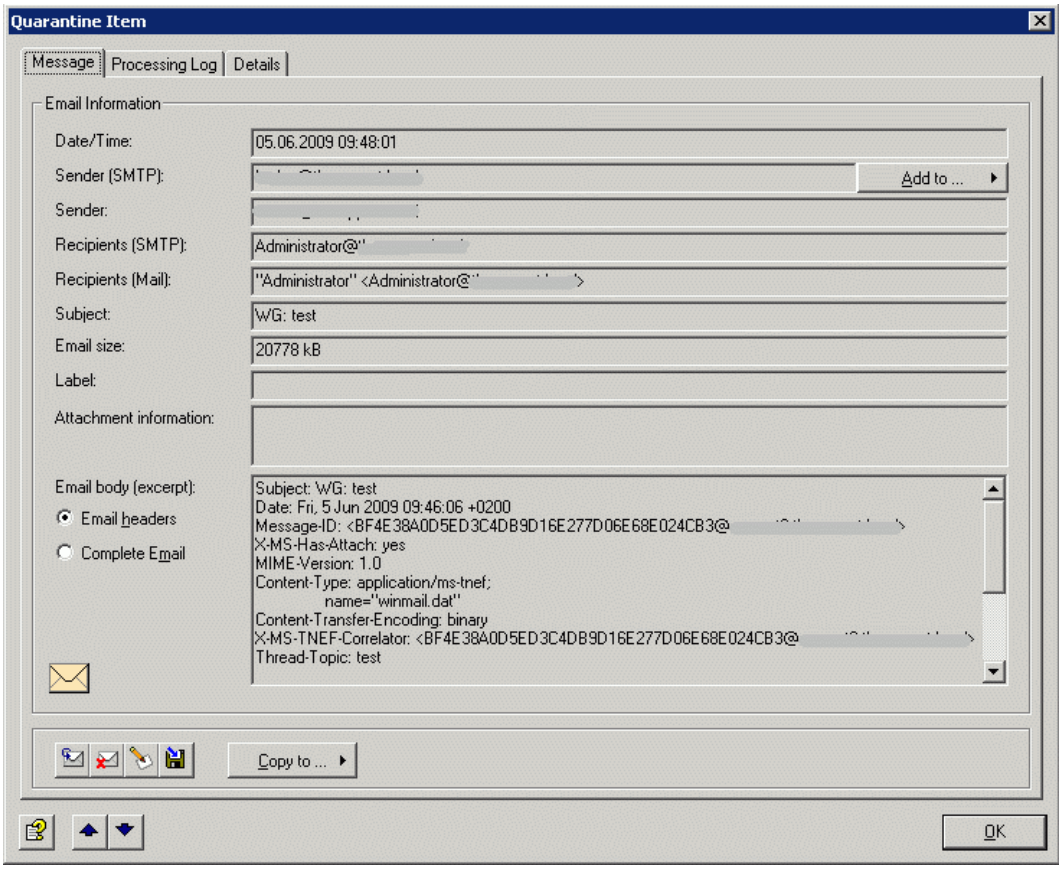
1. Under **Filter options**, select **No Filter**.
2. Right-click **View - Show all objects**.
3. Use the icon in the toolbar: .

The AntiVir Monitor view displays a maximum of 10.000 e-mails at a time (the most recent ones). To view older e-mails, select appropriate filter options to restrict the e-mails displayed.

A Quarantined Message

To view this information, double-click the quarantined message or right-click and select Properties of the quarantined e-mail.

The Message tab contains a summary of the important information:



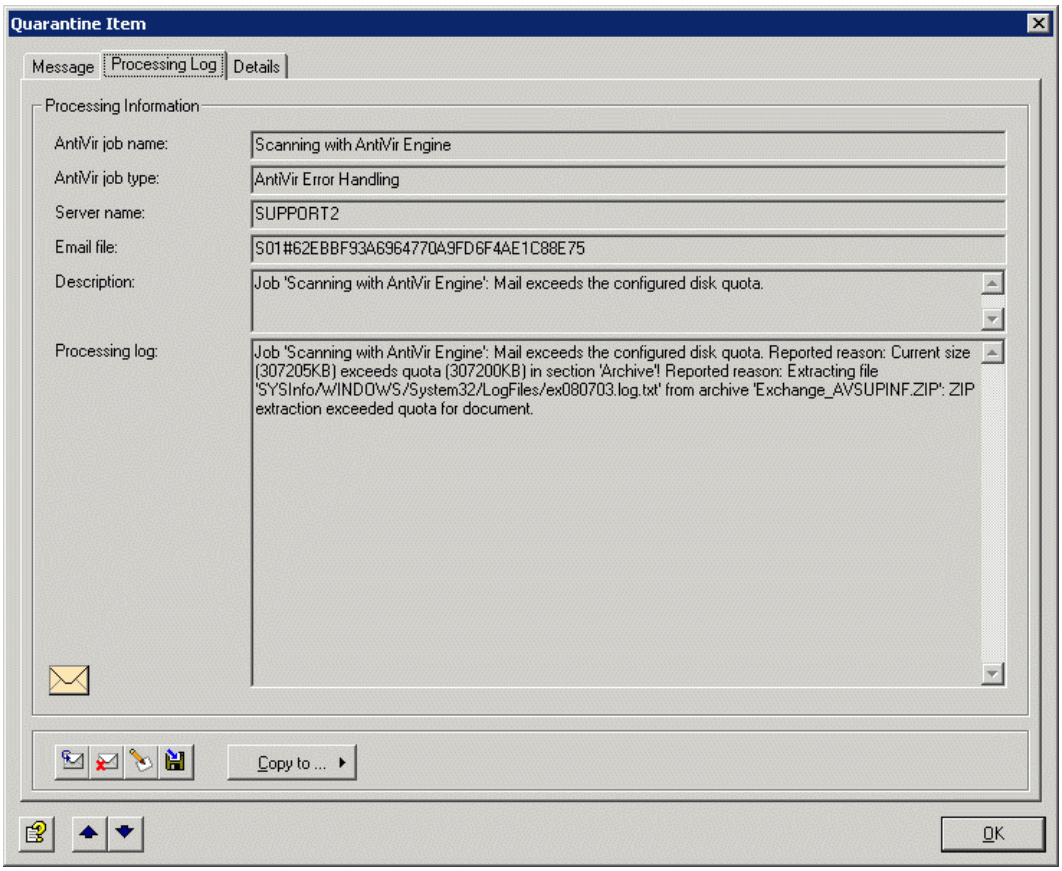
Icons used on these tabs:

	Send message from Quarantine
	Delete message in Quarantine
	Create, edit or delete message label
	Save message as
	Open Online Help
	Next message in Quarantine/badmail
	Previous message in Quarantine/badmail

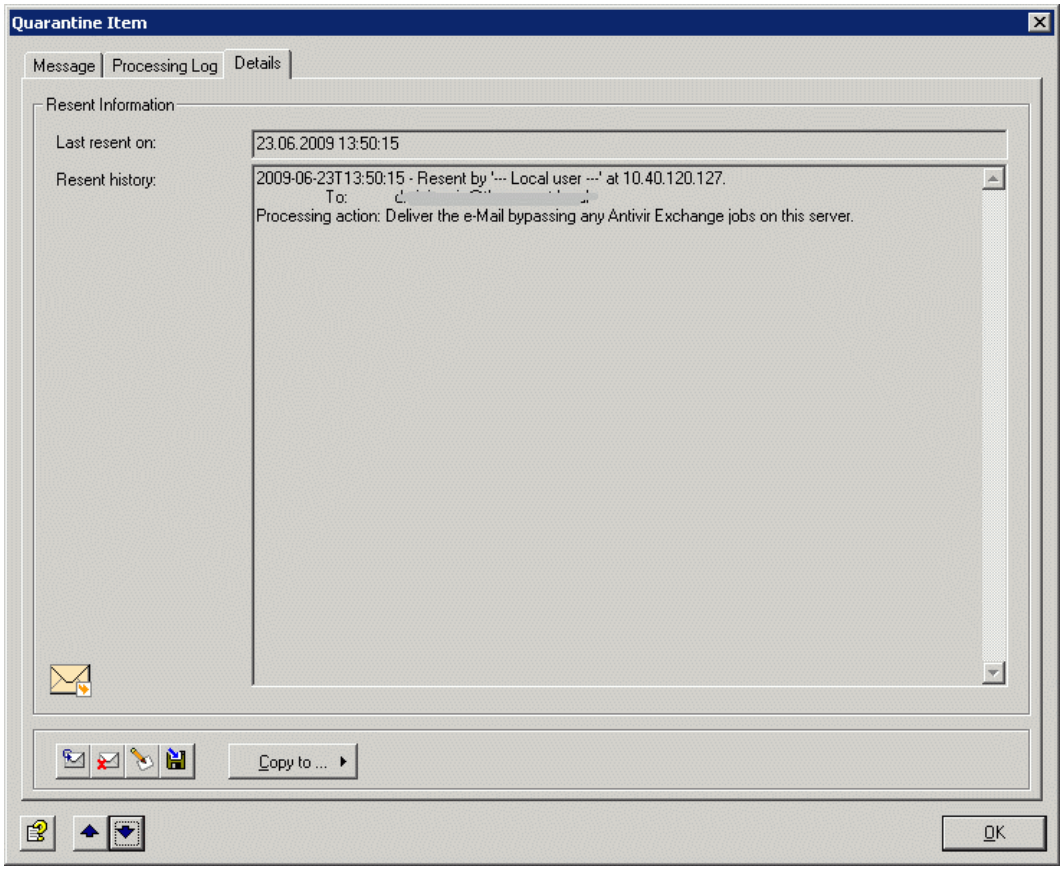
To add the message sender to an address list, click the **Add to** button. The address lists shown with this button are set individually. For further information refer to Address Lists . When you add the sender's address to the address list a message appears:

AntiVir Exchange Server 2000/2003
1 of 1 addresses are added.
(0 addresses already exists in Antispam: Whitelist,
0 addresses are invalid.)
OK

The **Processing Log** tab shows the name of the job that has quarantined the message, the job type, the server, the reason for quarantining the message as well as other processing details:


Quarantine Item
Message
Processing Log
Details
Processing Information
AntiVir job name:
Scanning with AntiVir Engine
AntiVir job type:
AntiVir Error Handling
Server name:
SUPPORT2
Email file:
S01#62EBBF93A6964770A9FD6F4AE1C88E75
Description:
Job 'Scanning with AntiVir Engine': Mail exceeds the configured disk quota.
Processing log:
Job 'Scanning with AntiVir Engine': Mail exceeds the configured disk quota. Reported reason: Current size (307205KB) exceeds quota (307200KB) in section 'Archive'! Reported reason: Extracting file 'SYSInfo/WINDOWS/System32/LogFiles/ex080703.log.txt' from archive 'Exchange_AVSUPINF.ZIP': ZIP extraction exceeded quota for document.
Copy to ...
OK

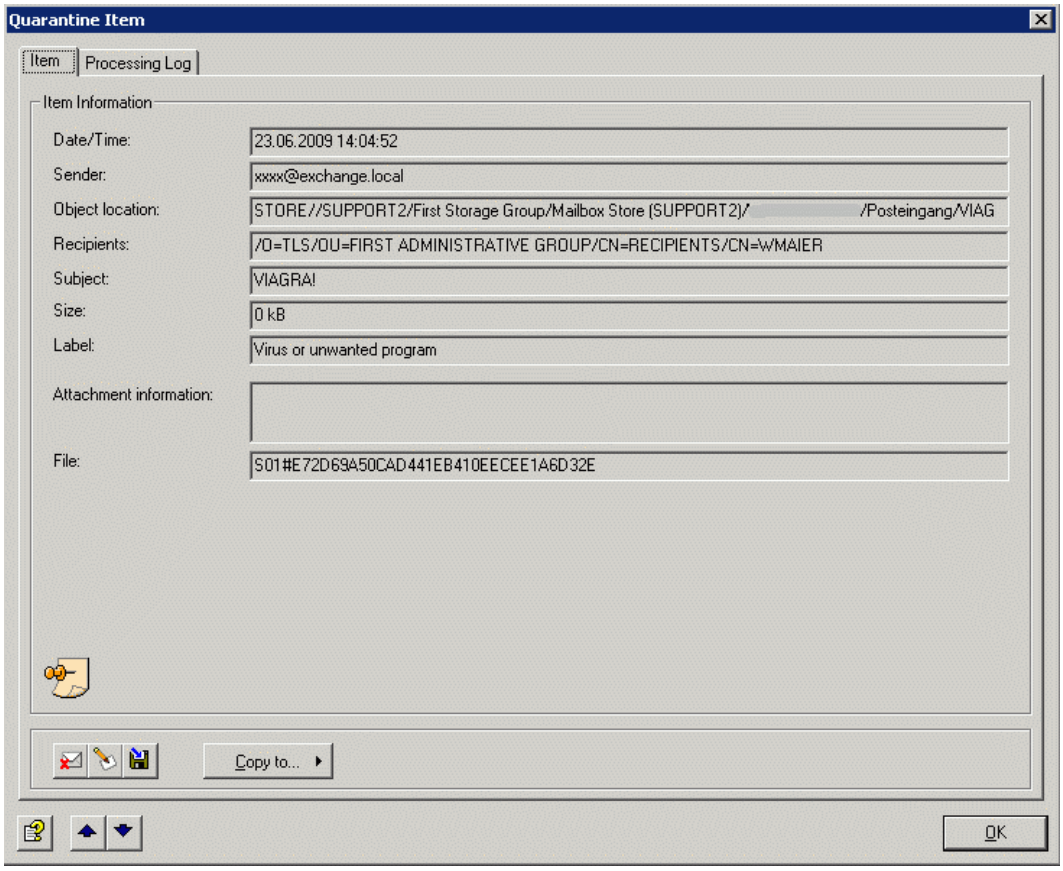
The **Details** tab displays **Resent information** (details on the resend process):



A Mail in the Information Store Quarantine

To view this information, double-click the message in the Information Store quarantine or right-click and select **Properties**.

The **Item** tab contains a summary of the important information:

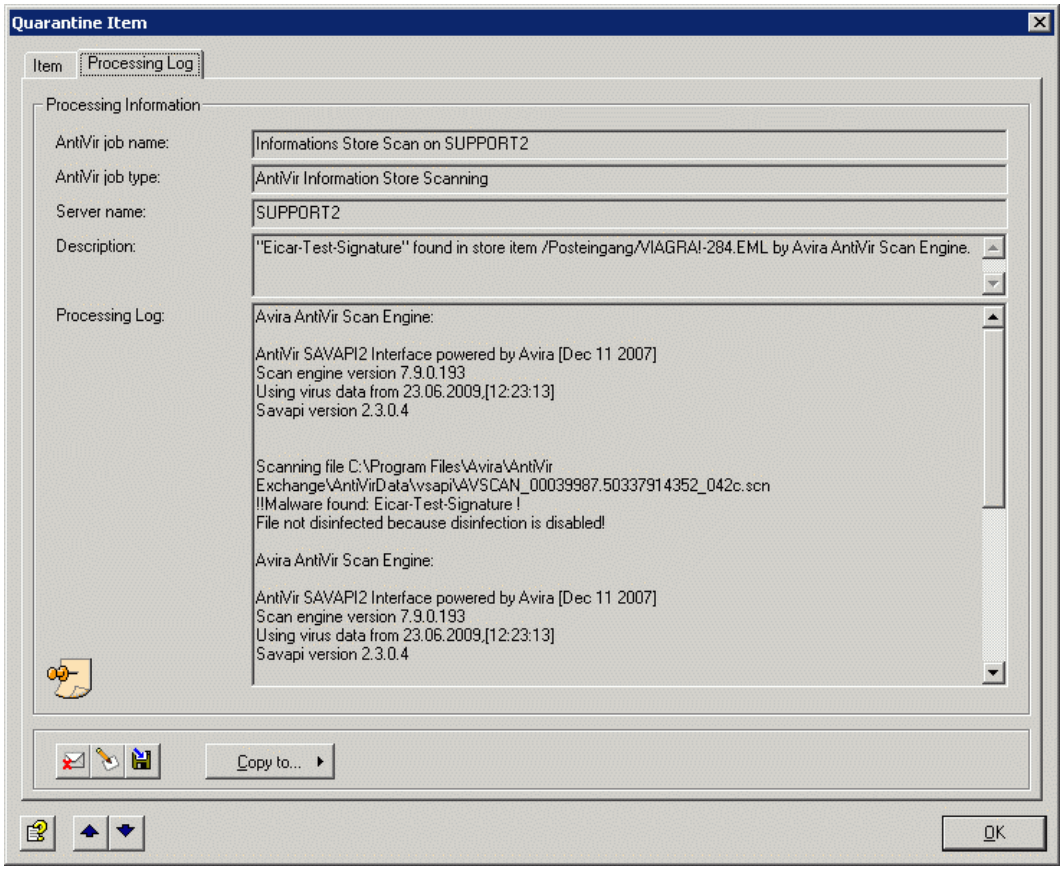


Icons used on these tabs:

	Delete item in quarantine
	Create, edit or delete item label
	Save item in the file system
	Next item in quarantine
	Previous item in quarantine

To copy the item to another quarantine on this server, right-click the item and select**All Tasks - Copy to**.

The **Processing Log** tab shows the name of the job that has quarantined the item, the job type, the server, the reason for quarantining the item as well as other processing details:



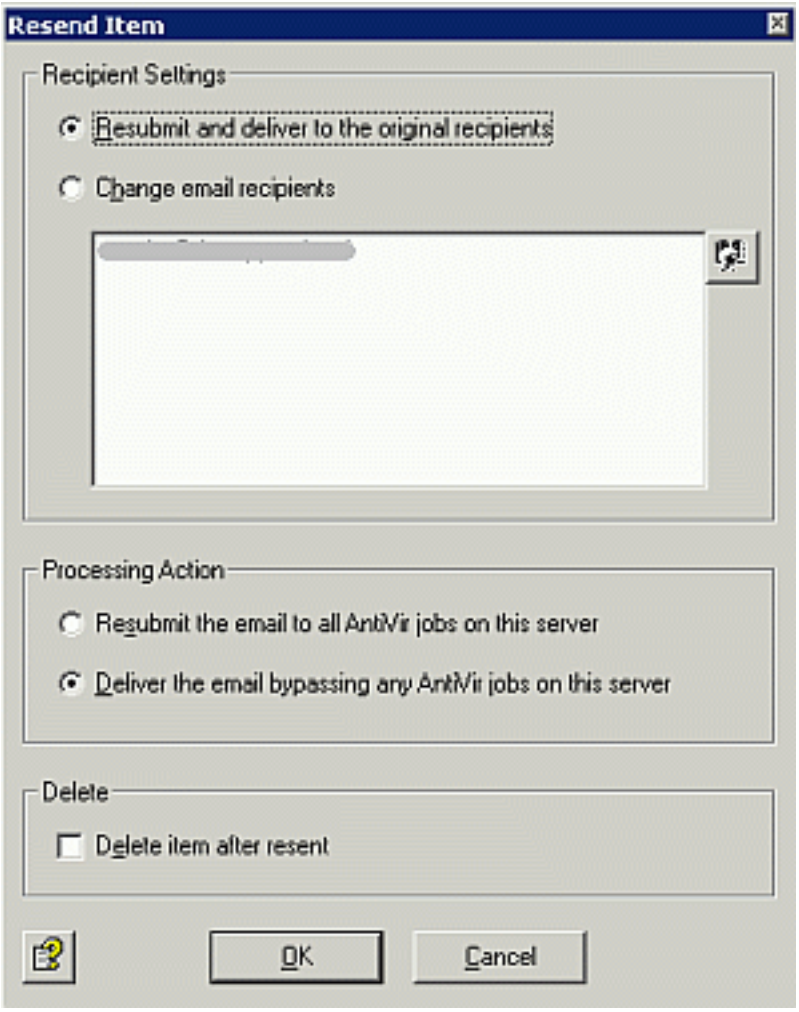
Sending From Quarantine

If you want to send a quarantined message to its original recipient or another user, you can resend it directly from the Quarantine without having it rechecked by the AntiVir Exchange job:

1. In the AntiVir Monitor, open a list of quarantined messages.
2. Right-click the desired message and select **All Tasks - Resend quarantine item**

Tip: *As an alternative, you can send the message directly from the Properties dialog by clicking the* *icon.*

The following dialog appears:



The From field of the message contains the original sender (i.e. not a forwarded mail).

3. To change the recipient, enable the **Change e-mail recipients** option and then click the **Select Address** icon: .

Note: *No address lists are available to select an address for resending from quarantine. Refer to Address Lists .*

4. If you do not want any jobs to process the message, select the option **Deliver the email bypassing any AntiVir jobs on this server**.

   When you forward a message from the Quarantine, it is likely to be urgent even though it contains restricted words or attachments, so you probably want this to be your default setting.

Note: *This is a global setting. If you have enabled jobs that are to scan mail resent from Quarantine, activate the option* ***Resubmit the email to all AntiVir jobs on this server****. Otherwise, the job option* ***Check emails resent from quarantine*** *will not apply and all messages will be forwarded without further checking.*
Note: *The instruction* ***Resubmit the email to all AntiVir jobs on this server*** *applies also to those jobs for which the option* ***Quarantined e-mails: Check emails resent from quarantine*** *has been enabled. This means that, even if you want quarantined e-mails to be processed again, all jobs for which the option* ***Ignore emails resent from quarantine*** *is selected will be excluded.*

Adding Senders to an Address List

If the e-mail of a specific sender has been quarantined, but you wish future mails from this sender to be accepted, you can add the sender to one of your address lists, e.g. `Anti-Spam: Whitelist`

1. In **Avira AntiVir Exchange Monitor**, open the Quarantine where the desired mail is located.
2. Right-click the mail and enable **All tasks - Add sender to addresslist**.
3. Select the address list to which the sender is to be added.

   If you want to make sure that all senders from a specific domain are accepted and let through to the recipients' mailboxes, proceed in the same way, but select the option **Add sender domain to addresslist**. This avoids having to add every single e-mail sender from a domain (e.g. a customer) to the address list individually. The address is added in the form `*@samplecompany.com`.

Note: *In both cases, the option* ***Allow adding addresses from quarantine*** *must be enabled within the address list. Otherwise the selected sender address cannot be added to the list!*

Bad Mail

Messages that cannot be processed by AntiVir jobs – such as messages with unknown formats – are referred to as "badmail". Because Avira AntiVir Exchange cannot read these messages, little is known about badmail. Such mail may therefore also contain undetected viruses.

There is only one badmail folder on each server, and you can not create further badmail folders. Otherwise, the same functions and options apply to badmail as for quarantined mail.

3.3.3.2 Avira AntiVir Exchange Reports

With **AntiVir Reports** functions, you can retrieve detailed information on e-mail processing. Eight predefined reports and one advanced statistics report are available.

The advanced statistics report can be defined individually.

The reports can be accessed through the AntiVir Monitor. The reports list the policy violations detected (e.g. viruses, undesired file attachments) both graphically and in list form. Specific reports are available for the most current Avira AntiVir Exchange issues. In addition, information on quarantines is also shown.

Reports can be created for freely selectable periods. They can be printed and exported with a wide range of options for further processing.

Report data is temporarily stored during processing and written to the evaluation database at half-hour intervals, i.e. processed e-mails do not immediately in the reports.

Click **AntiVir Reports** and double-click the required report in the right pane to open it. In the window that appears, enter the desired time span for the report. Click to export the analysis in one of several formats for importing into another application.

4 AntiVir

4.1 Overview

AntiVir checks messages for viruses, for the type and size of their attachments and for the total message size.

In that context, a distinction is made between scanning on the transport level (inbound/outbound messages) and scanning in the MS Exchange database (public and private Information Store).

Job types

- Virus scanning in inbound and outbound messages

  Job Type: **AntiVir Scanning**

- Virus scanning in MS Exchange databases (on access & proactive/background)

  Job: **Information Store scan**

- Blocking specific file types in attachments

  Job Type: **AntiVir Attachment Filtering**

- Limiting message size

  Job Type: **AntiVir Email Size Filtering**

- Limiting attachment type and/or size

  Job Type: **AntiVir Attachment/ Size Filtering**

Note: *Create a separate job for each restriction type! Job types cannot be changed later.*

For a detailed description of the procedure, refer to Enabling Virus Scanning - Example .

4.2 Virus Scanning

4.2.1 Scanning Inbound and Outbound Messages

To configure the scan engine, open the **Basic Configuration - Utility Settings**, right-click **AntiVir Engine** and edit the properties.

The job **Scanning with AntiVir Engine** starts the engine as defined in the configured conditions. The conditions determine the messages for which a job will be performed. If configured, further actions are performed as previously defined:

The example below illustrates the working principle of a virus scanning job. The job checks, for instance, an e-mail with the result “virus found”. It triggers a virus alarm and initiates a series of actions specified under **Actions**.

You can, for instance, specify the following:

1. If a virus is found, clean the original mail and deliver it to the recipient.
2. If the mail could not be cleaned, a copy of it is placed in your selected Quarantine

folder and the original is deleted without being forwarded.

3. Notifications with the relevant information from the scan engine and the AntiVir job are then sent to the Administrator, sender and recipient.

The following actions are possible:

- Scan for Viruses
- Clean infected message
- Add a subject extension
- Copy the entire e-mail to Quarantine
- Remove infected attachments from the message
- Delete the affected message without delivering it
- Run an external application
- Notify the Administrator, sender and/or recipient
- Notify any other, user-definable persons
- Add X-header field
- Redirect e-mail

4.2.2 Scanning in the Information Store

In addition to virus scanning at transport level, Avira AntiVir Exchange is also able to scan data in the public or private MS Exchange Information Store.

There are three basic types of Information Store scanning:

- **On-Demand scan**

  When a client tries to open a mail, a comparison is performed to ensure that text body and attachment have been checked by the current virus signature file. If they have not, the message is scanned before being forwarded to the client. On-demand scanning is the most commonly used task for Information Store scanning.

- **Pro-active scan**

  The proactive scan catches new messages before these are accessed by a client through an on-demand scan. Used in addition to on-demand scanning, it can help to speed up client access.

- **Background scan**

  A background scan checks all elements of the Information Store. It can be activated separately for the public and private Information Stores and scans all elements that were not yet scanned with the current scanner signature file.

In addition to a scheduled execution, the background scan is run whenever the database is loaded (for example when a server is started).

The Information Store scan is a global function that applies to the entire server, so that only one AntiVir Information Store scan job exists on each server (as opposed to any number of virus scanning jobs).

If a virus is found in a mail, various actions tailored to the Information Store scan can be performed:

- **block object**

  Object blocking denies access to the entire message object. Current Microsoft mail clients generate a message when the user tries to open a blocked message, while other and older clients may respond differently. The blocked message can always

be deleted, however.

- **replace with**

  You can replace infected elements with an information text. The infected element is then deleted.

- **mark as not infected**

  In exceptional cases, you may decide that an infected element is not to be flagged infected. Subsequent virus scans will then find the virus again. This action is intended for testing only, as it provides no protection for users and the system.

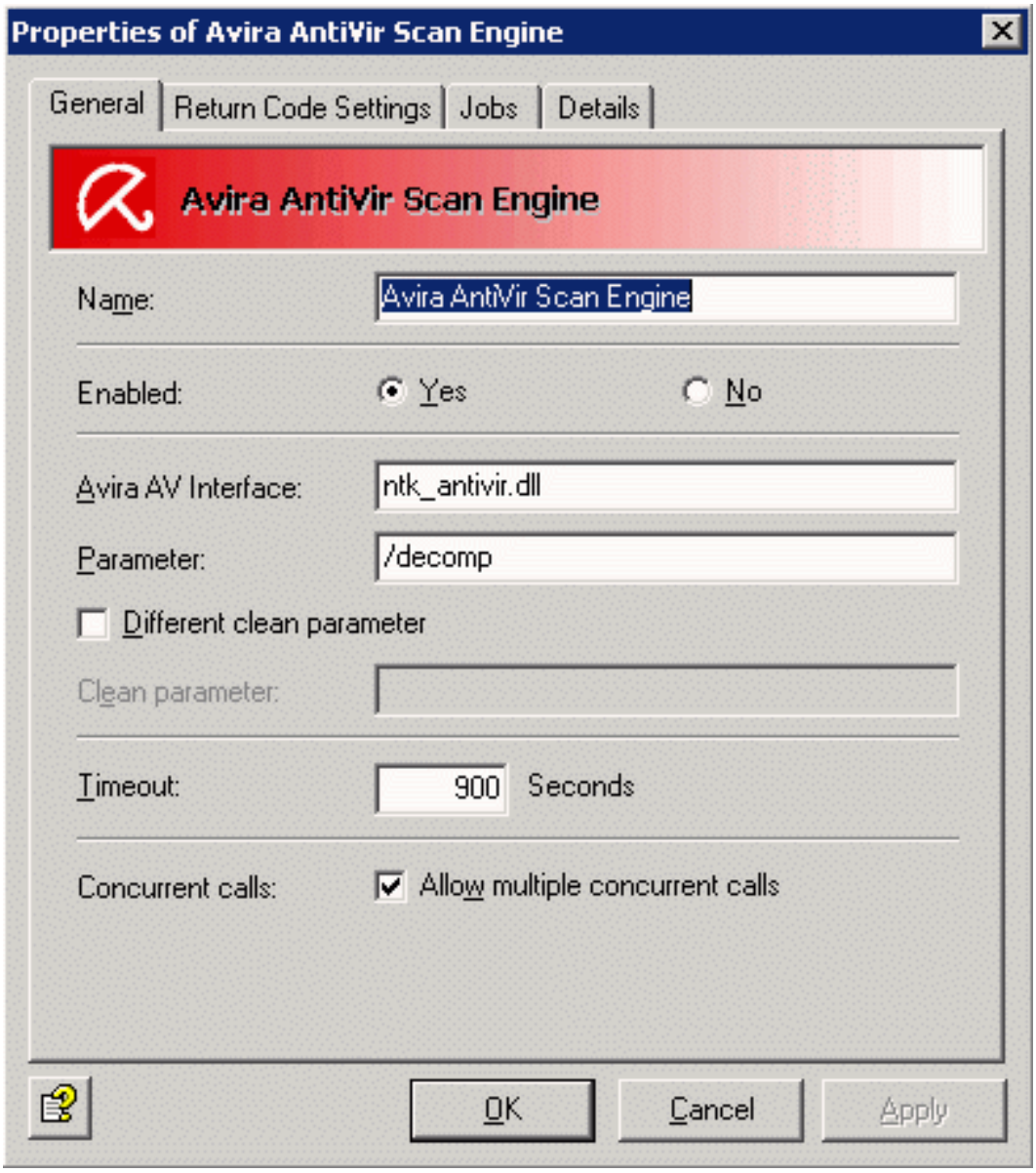
Note: *Virus scanning in the MS Exchange Information Store is performed by the Microsoft Virus Scanning API version 2.0/2,5. For further information, visit http://support.microsoft.com/kb/285667/EN/*
Attention: *Messages blocked by the Information Store scan may result in error messages during Information Store backups.*
Attention: *Exiting or uninstalling Avira AntiVir Exchange and terminating the Information Store scan jobs releases any elements that were blocked due to virus infection as well as disabling the Information Store's active virus protection.*

4.2.3 Configuring and Enabling the AntiVir Scanner

Except for the AntiVir scan engine, we do not supply any virus scanners. Avira AntiVir Exchange calls the scan engine through the **Avira AV Interface** - a DLL file.

Attention: *Disable any real-time or on-access scan functions of your scan engines for the* `...\Avira\AntiVir Exchange\AntiVirData\` *directory.*

Test your scan engine for correct operation: Under **AntiVir Monitor**, select the desired server name and, in the right pane, click **Server Status**. Under the **Scan engine Test** tab, click on **Start**. If successful, an OK is returned along with a message saying that an EICAR test virus was found.



You can change the properties of the scan engine under **Basic Configuration - Utility Settings - AntiVir Engine - Properties**.

- The name of the Avira antivirus interface DLL must be entered in the **Avira AV Interface** field. This DLL file represents the link between Avira AntiVir Exchange and the virus scanner. This entry is pre-configured for all scan engines and must not be changed! In the **Parameter** field, enter the parameter to be used by the virus scanner for scanning.
- To configure the virus scanner so that e-mails or attachments are cleaned when a virus is detected, enable the **Different clean parameter** option and enter the appropriate parameter in the **Clean parameter** field underneath.

Note: *If you wish to use the scan engine for virus checking only, use the AntiVir job* ***Scanning with AntiVir Engine*** *and disable the* ***Remove malware*** *option in the* ***Actions*** *tab. If the virus scanner is to clean any infected files found, use the AntiVir job* ***Scanning and disinfection with AntiVir Engine****. In this case, the option* ***Remove malware*** *needs to be enabled and the actions to be performed for infected mails must have been set.*

- **Update timeout**:

  Enter the number of seconds after which an unsuccessful attempt to connect to the server is aborted. Take into account the performance of your server. The minimum value is 60 seconds. We recommend a value of 60 to 120 seconds.

- **Allow multiple concurrent calls**:

  Sets that the scan engine can process several e-mails at the same time. The specific number of calls is set under **Basic Configuration - AntiVir Server - Properties - General** tab: **Number of threads**. Also refer to Settings for an Individual Avira AntiVir Exchange Server .

The **Return Code Settings** tab can be used to edit the pre-configured return codes. The meaning of each code is to be found under **Details - Comments**.

The **Jobs** tab lists the jobs that use the scan engine.

Attention: *Please do not use this tab for updating Avira AntiVir Exchange.*

AntiVir powered by Avira

The AntiVir Engine is included in the installation package and is enabled by default.

Default parameters:

- `/decomp` (decompress PKLite and LZExe archives)
- `/verbosescan` (scan complete file)

Alternative parameter:

- `/paranoid` (interpret warning from heuristic analysis as virus)

If you are using a proxy server, specify the `savapi.ini` file for online updates in the Setup. To change the file at a later stage proceed as follows:

1. Stop the SAVAPI service.
2. Go to the folder `Avira\ AntiVir Exchange\Engine\`.
3. Open the `savapi.ini` file with Notepad.
4. Set the following parameters:

Use proxy server for updates	**If this value is enabled (1), the engine tries to download the updates through the specified proxy. By default, no proxy server is used. Example: `ProxyEnabled=0` (=not enabled).**
Proxy server address	**Use this parameter to enter the full name or IP address of the proxy server used for the update. This value is used only when "ProxyEnabled" is enabled. Example: `ProxyUrl=proxy.mydomain.de`**
Proxy port address	**The port specified here is used for updates through the proxy server. This value is used only when "ProxyEnabled" is enabled. Specify the port number of the proxy server in this parameter. Example: `ProxyPort=3128`**
User name for proxy server (proxy authentication)	**Use this parameter to enter the user name under which the update service logs on to the proxy server. This value is used only when "ProxyEnabled" is enabled. Example: `ProxyUserName=fmaier`**

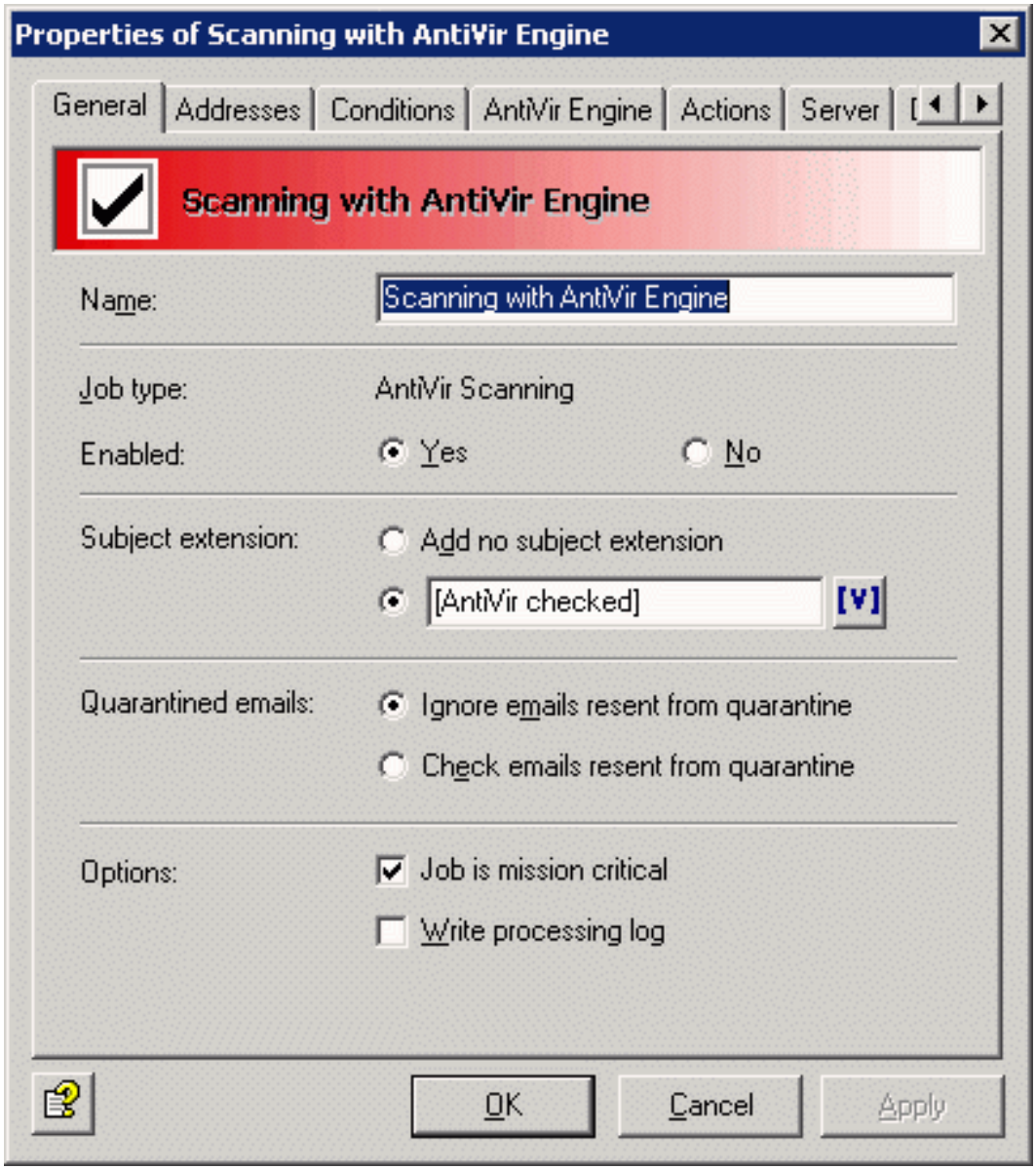
Password for proxy server (proxy authentication)	**Use this parameter to set the password to be used by the update service along with the user name to connect to the proxy server. This value is used only when "ProxyEnabled" is enabled. Example: `ProxyPassword=passwort`**
Search interval for new updates	**This value specifies the number of minutes after which the update service searches for new versions on the server entered under UpdateURL. The default value is 120 minutes (2 hours). An automatic update of the engine and virus signatures is automatically performed immediately after the first action (virus scan). If this value is zero, automatic updating is disabled. Example: `UpdateInterval=120`**

4.2.4 Enabling Virus Scanning - Example

Under **Policy Configuration - Mail Transport Jobs**, you will find the **Scanning with AntiVir Engine** job. Double-click this job to open it.

General Settings

Under the **General** tab, enter a name for the job. Each enaled job has a checkmark in the job symbol. To enable a job, select **Enabled: Yes**. Once you have saved your settings with **Apply** and closed the job, the job is enabled.



By default, the **Subject extension** is pre-set to **AntiVir checked**. This text is added to the subject of each mail checked by the job.

This job also processes **Quarantined emails**. The processing action for sending from quarantine applies to all jobs and has priority. Therefore, if you select an email in the AntiVir Monitor and use the **Resend item** command, with activated option **Deliver the email bypassing any AntiVir jobs on this server**, the email is not processed by any job. So you should use the option **Resubmit the email to all AntiVir jobs on this server**.

For further information on sending quarantined mail refer to Sending From Quarantine .

Job is mission critical

If a job is **mission-critical**, any errors would place the email in the badmail area. Enable this option for critical jobs such as virus scanning (select checkbox).

Attention: *Until the cause is rectified,* ***all*** *affected e-mails, both inbound and outbound, are placed in the badmail area!*

A job is **not mission-critical** when any processing errors are to be ignored for the corresponding e-mail, in which case it is passed to the next job for further processing. All processing errors are recorded in the Windows Event Log. If the same processing error occurs five times in succession, the job is disabled and automatically restarted after 15 minutes. Do not enable this option for company-critical jobs.

For most of the jobs, the default setting is **not mission-critical**. The jobs to be considered mission-critical should be defined through corporate policies.

Write processing log

The Processing Log provides information on how e-mails were processed by the job. Enable this function if you need some sort of evidence or if you wish to test the job.

With this option enabled, information on whether and how the job has processed the mail is written into a text file for each mail. This log text file is stored in the Avira AntiVir Exchange installation directory in the `Log` folder. Logging is defined for each job, but the text file contains the information for all jobs for which **Write processing log** is enabled. A separate text file is created for each day.

Name of the text file: `Audit_all_<date of last modification>.log`, e.g. `Audit_all_20050909.log`

Individual pieces of information on the e-mail processed are separated by semicolon and can be evaluated manually or automatically:

1. Date and time when the e-mail was processed
2. Job ID
3. Job name
4. Message ID
5. SMTP sender
6. SMTP recipient
7. Avira AntiVir Exchange filtering result
    a. Restricted - e-mail matches the restrictions defined
    b. Unrestricted - e-mail does not match the restrictions defined

Recipient groups are resolved, with a separate line written for each recipient.

Setting up Address Conditions

Under the **Addresses** tab, specify the senders or recipients to which this job is to apply. You can select addresses from existing lists or from your own ones. For details on how to make the best use of address lists and details, refer to the description under Address Lists .

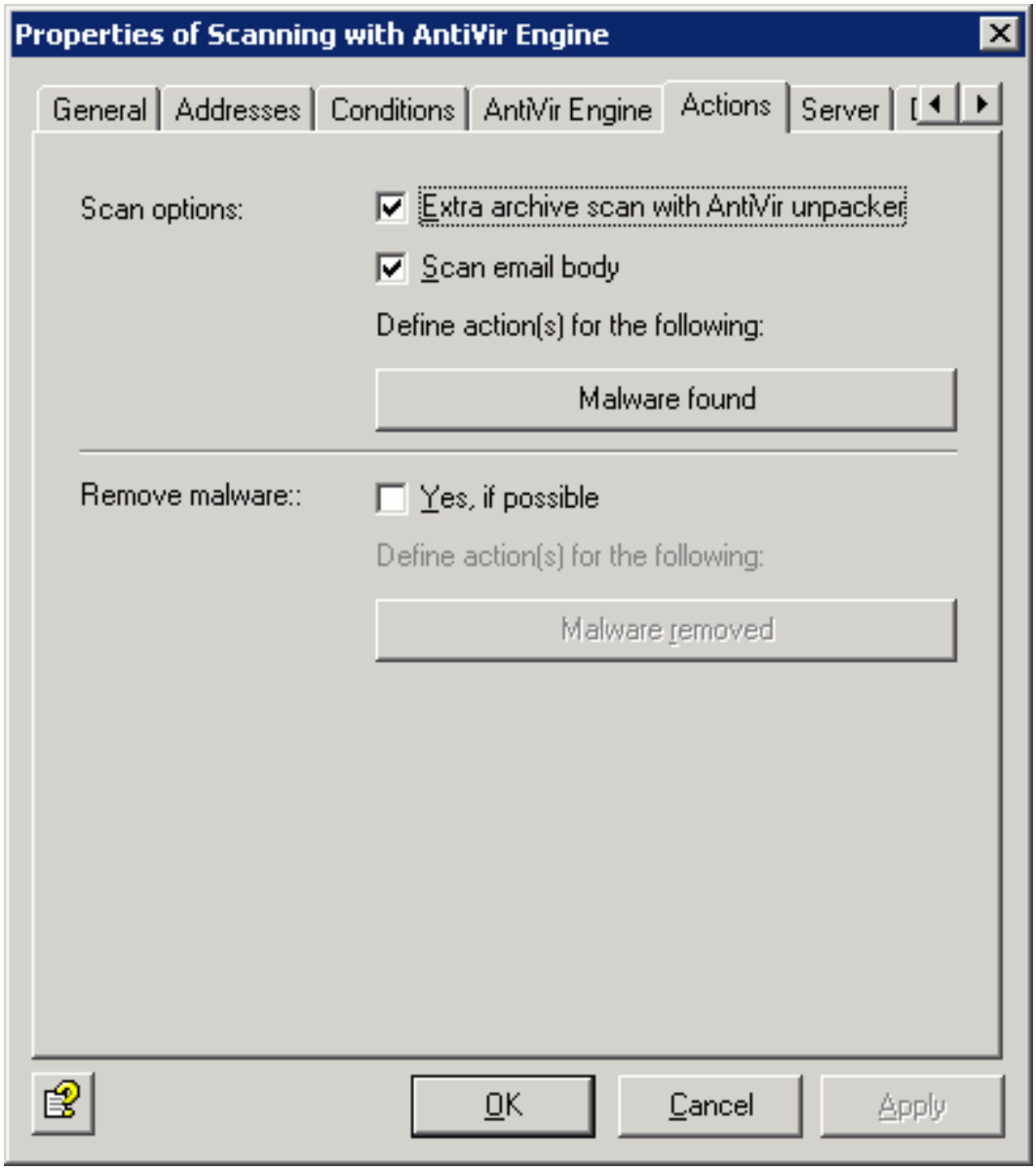
Setting up Content Conditions

Under the **Conditions** tab you can set the requirements as to which mails or documents a job is to be run for. For the use and settings of conditions refer to Conditions .

Note: *The content conditions and the address conditions set in the* ***Addresses*** *tab must simultaneously come true, for a job to be run (logical AND).*

Defining Actions

Under the **Actions** tab, specify the actions to be taken **when the job finds a virus-infected message**:



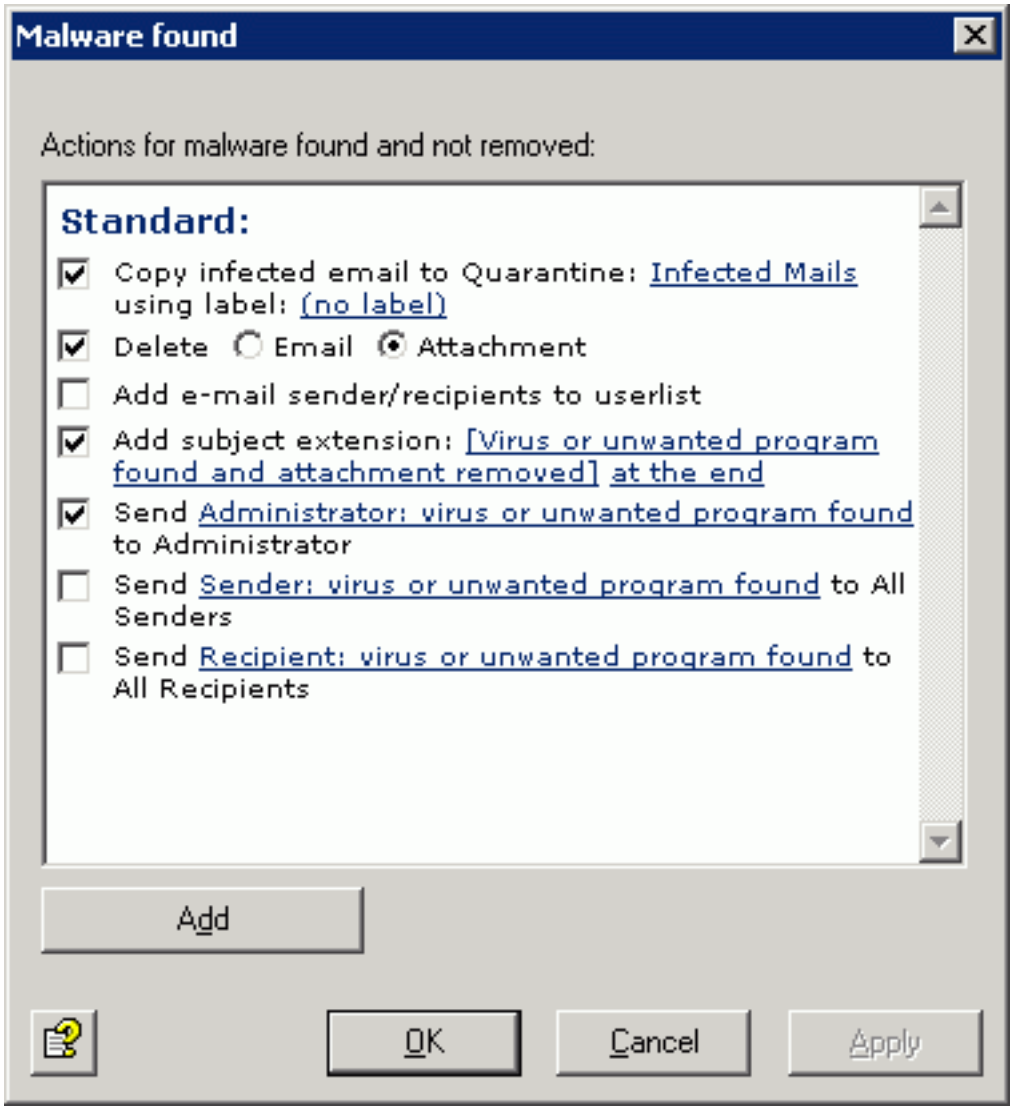
This job scans e-mails for viruses but does not attempt to clean infected e-mails and attachments. Although the virus scanner is capable of cleaning infected objects, it is advisable to quarantine infected attachments immediately, as, in practice, viruses are usually received in spam and rarely by accident from known communication partners.

Note: *As the job is to perform a virus scan only, you need to configure the scan engine accordingly. Under* ***Basic Configuration - Utility Settings - AntiVir Engine****, select the engine and disable the* ***Different clean parameter*** *field. Enable this field if the job is to clean an infected mail or attachment.*

After you have defined what is to be checked, specify two different actions:

1. One to be performed in case a virus was found and the file could not be cleaned,
2. and another in case the file was cleaned successfully (if you have selected this option).

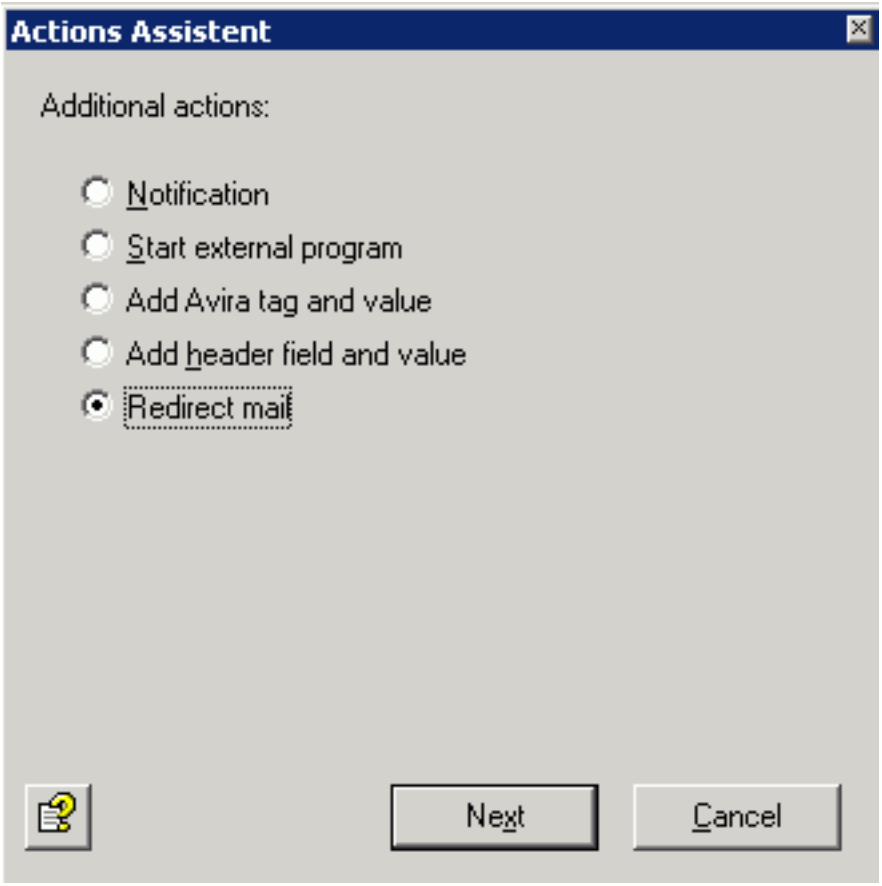
The configuration of the actions is the same in both cases. The following examples illustrates the fist case:


Malware found
Actions for malware found and not removed:
Standard:
Copy infected email to Quarantine: Infected Mails using label: (no label)
Delete Email Attachment
Add e-mail sender/recipients to userlist
Add subject extension: [Virus or unwanted program found and attachment removed] at the end
Send Administrator: virus or unwanted program found to Administrator
Send Sender: virus or unwanted program found to All Senders
Send Recipient: virus or unwanted program found to All Recipients
Add
OK
Cancel
Apply

In this example, a copy of the e-mail is placed in Quarantine and the infected attachments are deleted. The message is delivered to its recipient only if the message body is virus-free and the attachment could be deleted. A notification on the virus is sent to the Administrator. You can select this notification from the list menu of available notification templates, which you can format using the HTML toolbar or by directly entering appropriate HTML code.

Tip: *Check whether the infected mails addressed to your company are often also spam. If they are, it is best to delete the entire message and not just the attachment. This saves filtering of the remaining message text.*
Note: *If you have selected the* ***Scan options: Scan e-mail body*** *option and a virus is found in the text body, the entire message including any attachments is deleted if you have selected the* ***Delete and don't deliver the restricted attachment(s)*** *option (attachments are not delivered without text body). The affected message section is usually deleted separately. If only the attachment was infected, only the attachment is deleted.*

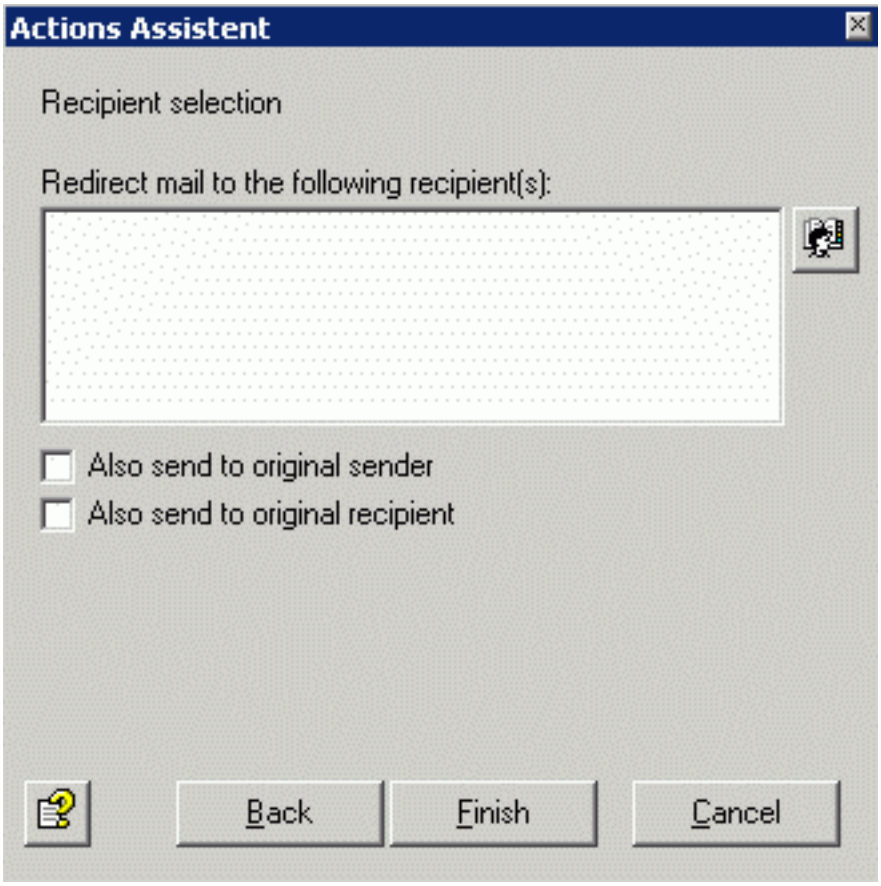
To define additional actions click **Add**:



- **Notification**: Select the recipient of the notification from the address book.
- **Start external program**: Define a new application to perform actions of this application. To start an external application enter the path and, where required, any necessary parameters.
- **Add Avira tag and value**: Mail header tags can be inserted by Avira AntiVir Exchange during the process in order to perform special Avira AntiVir Exchange actions. For instance, it is possible to add information to an e-mail that can be evaluated by a subsequent job. When the e-mail is sent to its original recipients, the information in the mail header tag is removed.
- **Add header field and value**: Define a new X header field and select the variable to be inserted, e.g. to return a spam analysis result as code or value. As opposed to the mail header tag this information is not removed when the e-mail is sent to its original recipients.
- **Redirect mail:** Select the recipient of the redirected mail from the address book. The Redirect mail option is not enabled by default, it is simply included as additional suggestion.

Note: *About* ***Redirect mail*** *- When you redirect a TNEF message to an external address, the recipient will get a blank message that may contain an attached file called* `winmail.dat`*. Exchange uses the TNEF format when an Outlook user (not Outlook Express!) sends a message within an Exchange organization. This format is not used for Internet communications or by other mail programs.*

Click **Next** and make additional settings (depending on the options selected). In the case of **Redirect mail** the following options are available:

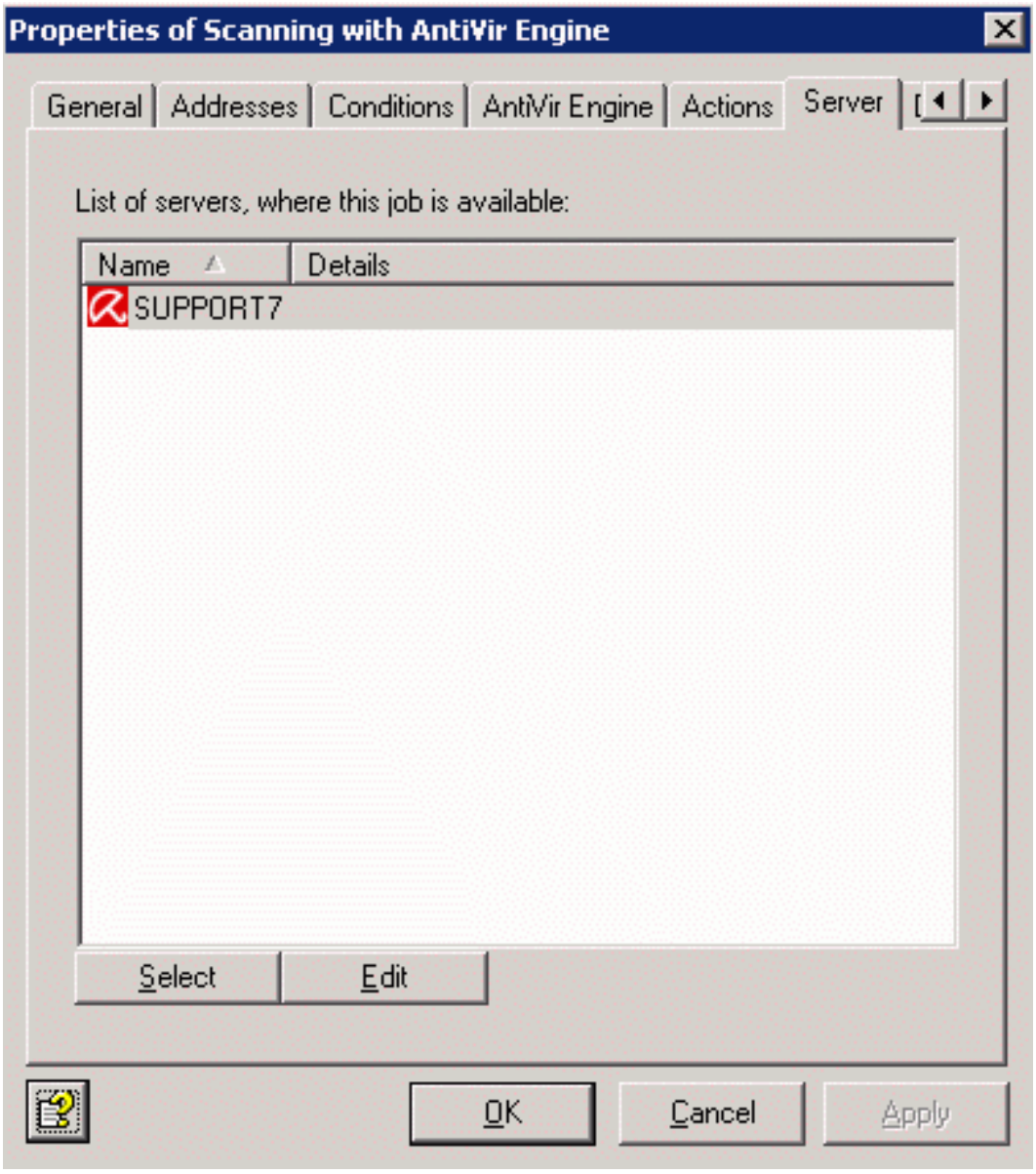


Click the address book icon to select further recipients or define **own addresses**. If the e-mail is also to be delivered to the **original recipient** or **original sender**, enable the corresponding checkbox.

After having entered the recipient click **Finish**.

Selecting Servers

Under the **Server** tab, select the server or servers on which the job is to be enabled.



Click **Select**. A dialog similar to the one for selecting scan engines appears.

Note: *If a server is not listed, it may not be correctly configured. For further information about configuring Avira AntiVir Exchange servers refer to Settings for an Individual Avira AntiVir Exchange Server .*

Entering Job Details

Use the **Details** tab to add a job description.

Save the configuration of the AntiVir Exchange Management Console each time you have modified the settings. Click on the **Save** button . The configuration is saved in the `ConfigData.xml` file located in the `Avira\AntiVir Exchange\Config` folder. Pending changes are indicated by an asterisk (*) next to the top node.

4.3 Virus Scan in the Information Store - Sample Job

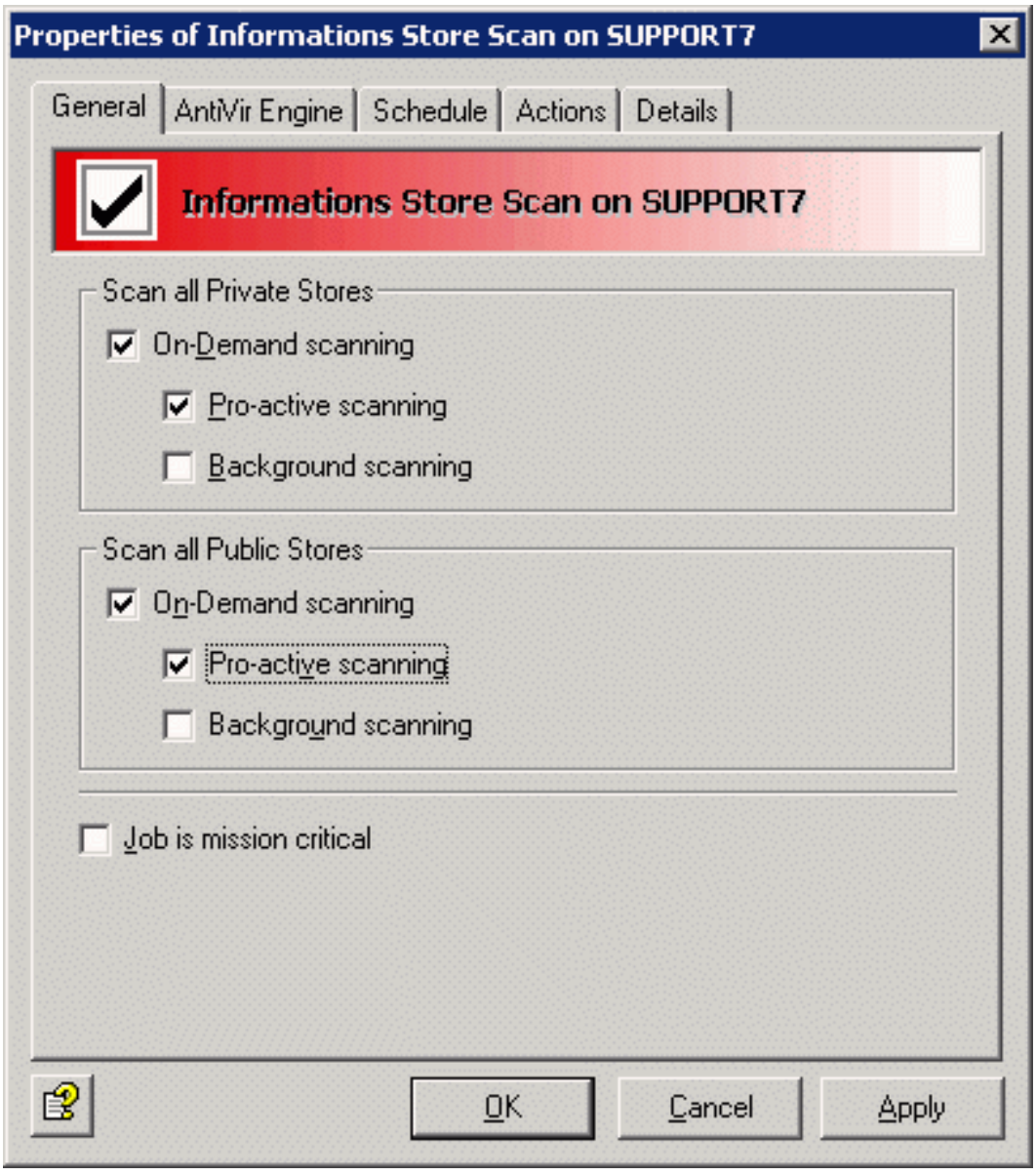
Under **Policy Configuration** in the **Information Store jobs** area, you will find an **Information Store scan** job for each server. Double-click this job to open it.

Attention: *When you enable or disable the Information Store scan job, it takes up to two minutes for the Exchange Store to register the change.*

4.3.1 General Settings

Under the **General** tab you can enable on-demand scanning for both the private and the public Information Store.

In addition to on-demand scanning, you can also enable proactive and background scanning. For further information, refer to Scanning in the Information Store .

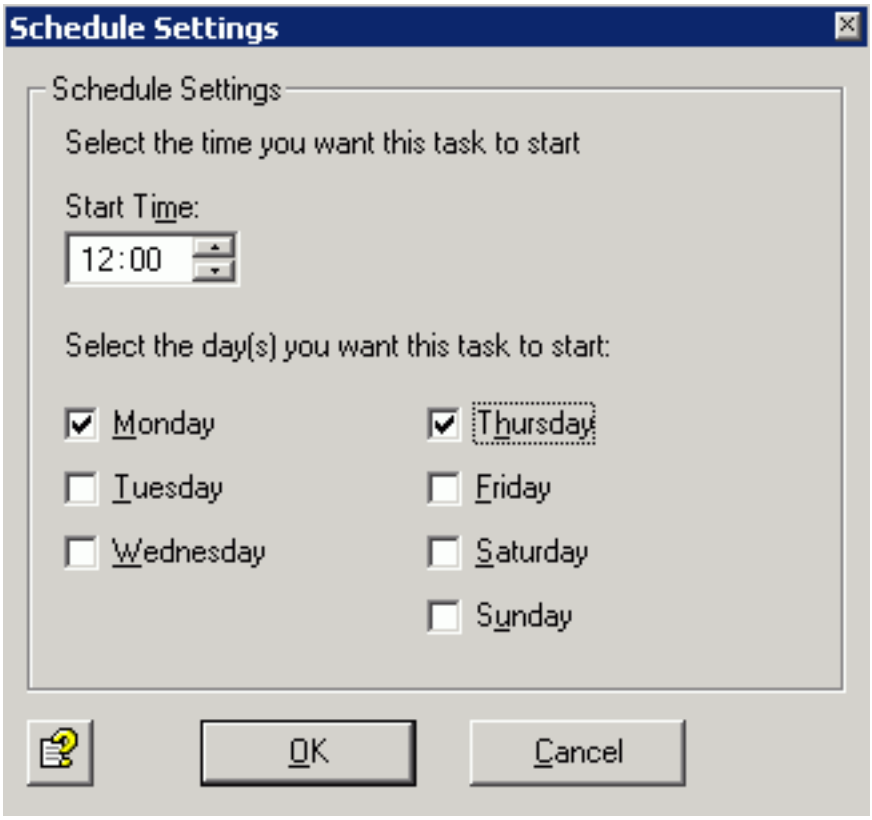


For details on the **Mission Critical** option, refer to This job is mission-critical

4.3.2 Scheduling

Use the **Schedule** tab to define a schedule for restarting the scan. When scanning is restarted, all elements in the Information Store are checked one more time. This applies to all three scan modes. If you have enabled background scanning, this scan may take a long time and use a lot of processor capacity. It is therefore advisable to restart scanning during periods of low system usage and following pattern file updates.

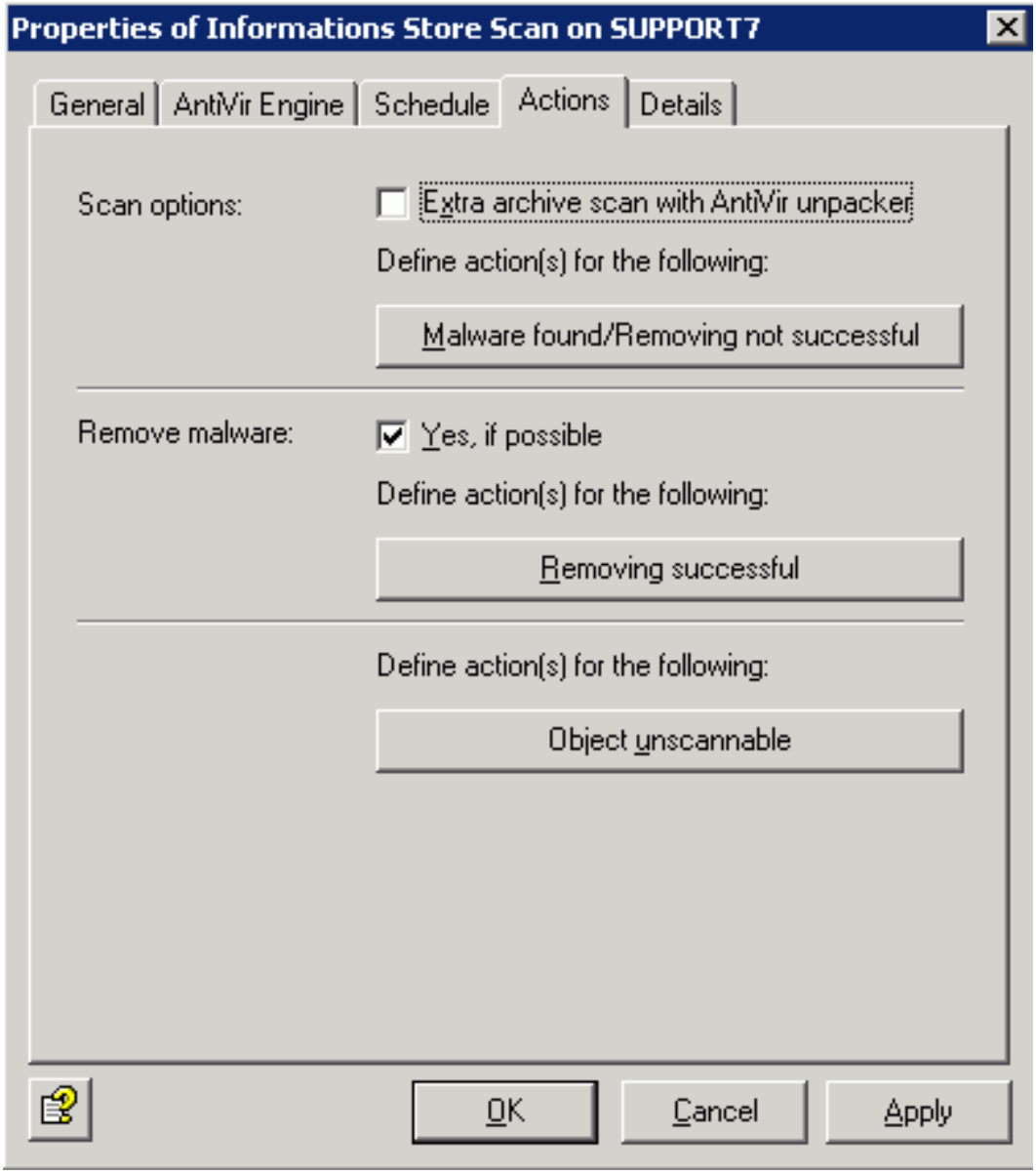
To create a schedule entry click **Add**. Then select a start time and the days on which restarting is to be performed. Confirm with **OK**.



4.3.3 Defining Actions

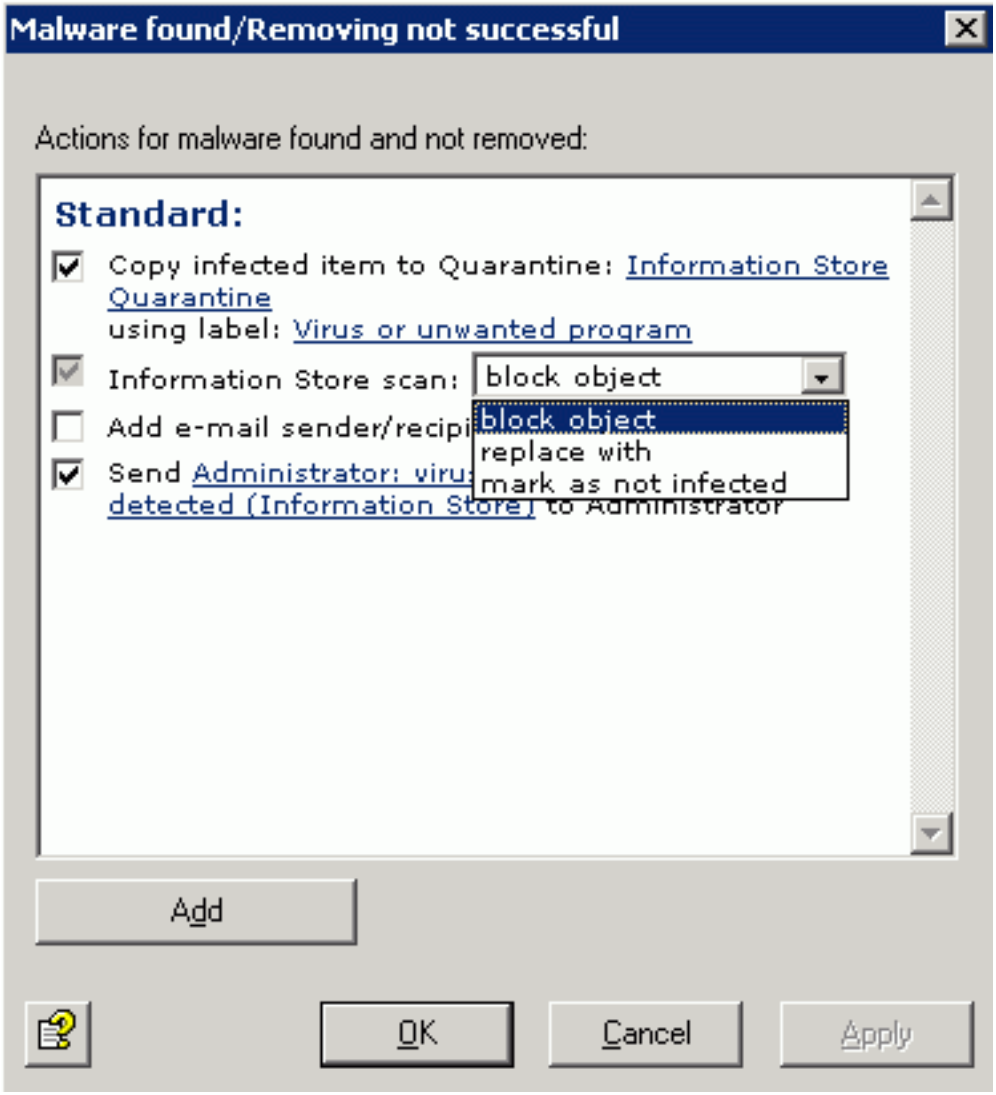
Under the **Actions** tab, specify the actions to be taken if the job finds an infected mail.

Extra archive scan with AntiVir unpacker: Avira AntiVir Exchange's built-in unpacker will extract the compressed files before passing them to the virus scanner.



Three different actions are possible:

1. **Virus found/Removing not successful**: Specifies the actions if virus was found and the file could not be cleaned.



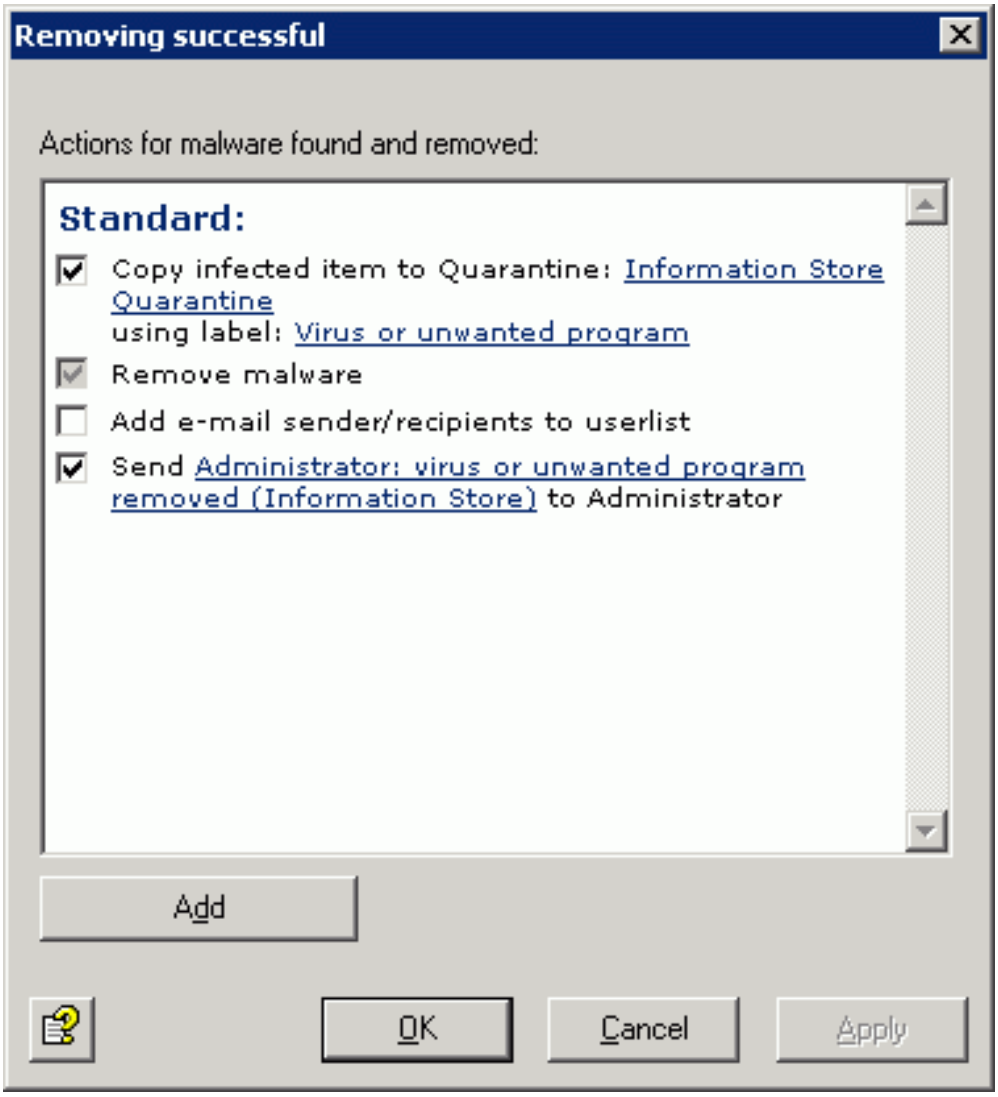
a. Specify whether a copy of the object is to be quarantined and labeled. A separate default quarantine is available for the Information Store.

b. With the second option, the object can be blocked, replaced or just marked as not infected. Also refer to Scanning in the Information Store .

c. The final option defines whether a notification is sent to the administrator(s).

d. Use the **Add** button to define further actions, for instance sending notifications to other users or starting an external application.

2. **Removing successful:** Specifies the actions to be taken if the file was cleaned successfully.

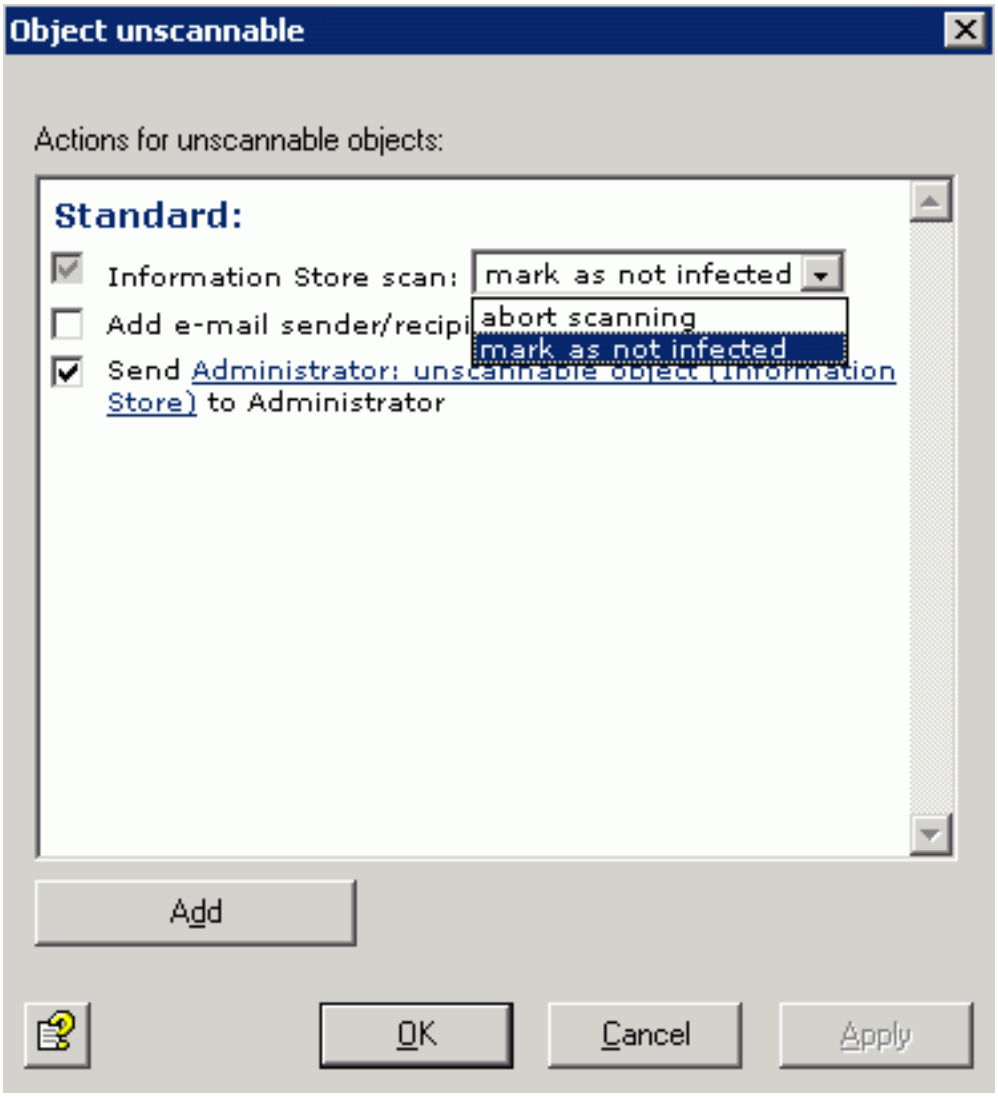


The following actions are available:

a. Use the first option to specify whether a copy of the object is to be quarantined and labeled. The copy is created before cleaning so that the object is quarantined in its original state.

b. In addition you can define whether a notification is sent to the administrator(s).

3. **Object unscannable**: This option allows to control the behavior of Avira AntiVir Exchange when it finds encrypted objects, which cannot be opened for scanning.



Two options are available. In the **Information Store scan** field, select one of two settings:

a. **abort scanning**: The object will be rescanned with the next scan. If previous scans have not treated the object as uninfected, access is denied.

b. **mark as not infected**: The object is treated as if it were virus-free. It is not rescanned before virus scanning is restarted.

You can also notify the administrator and add further actions by clicking on the **Add** button.

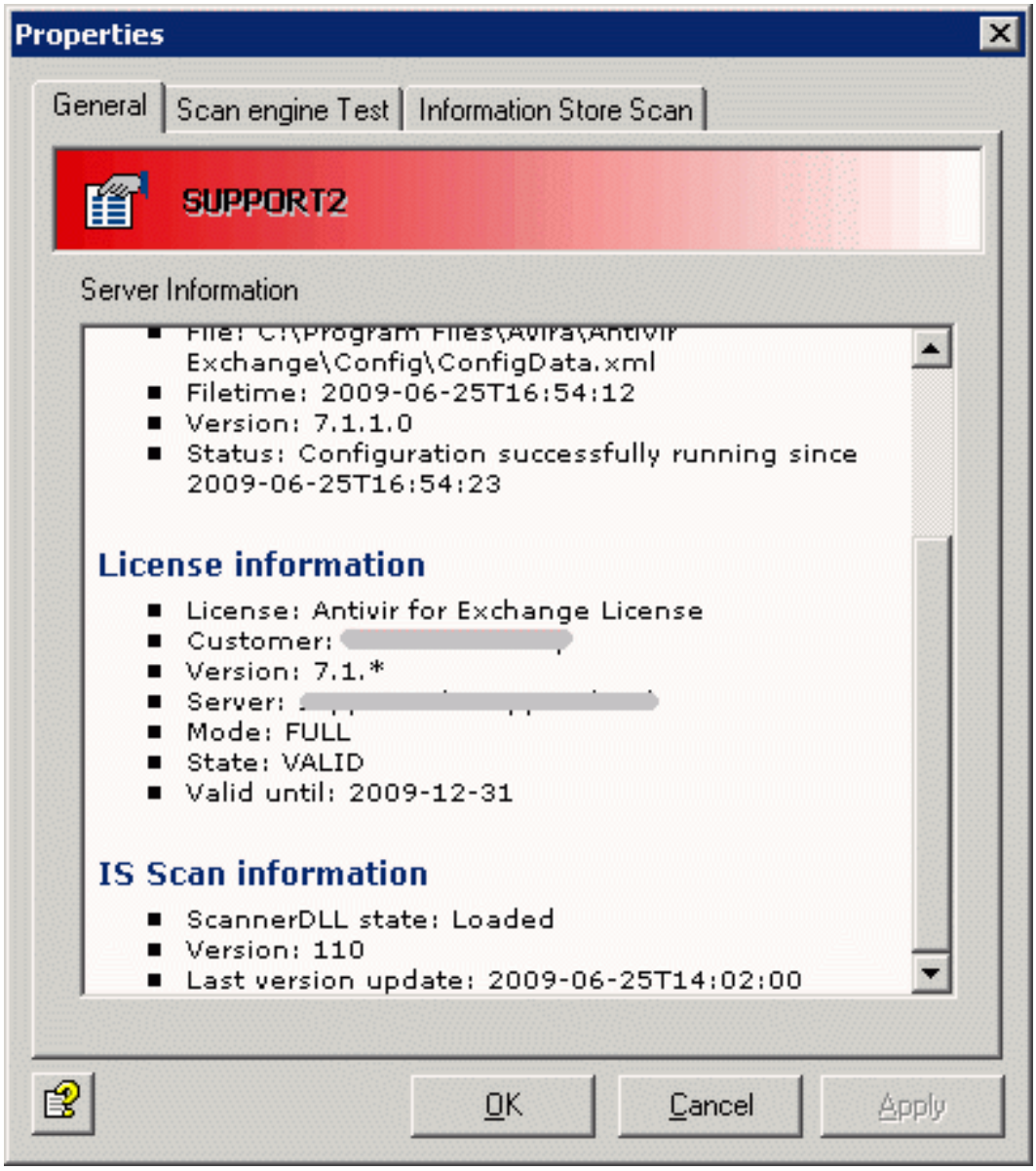
4.3.4 Job Details

Refer to Entering Job Details .

4.3.5 Server Status

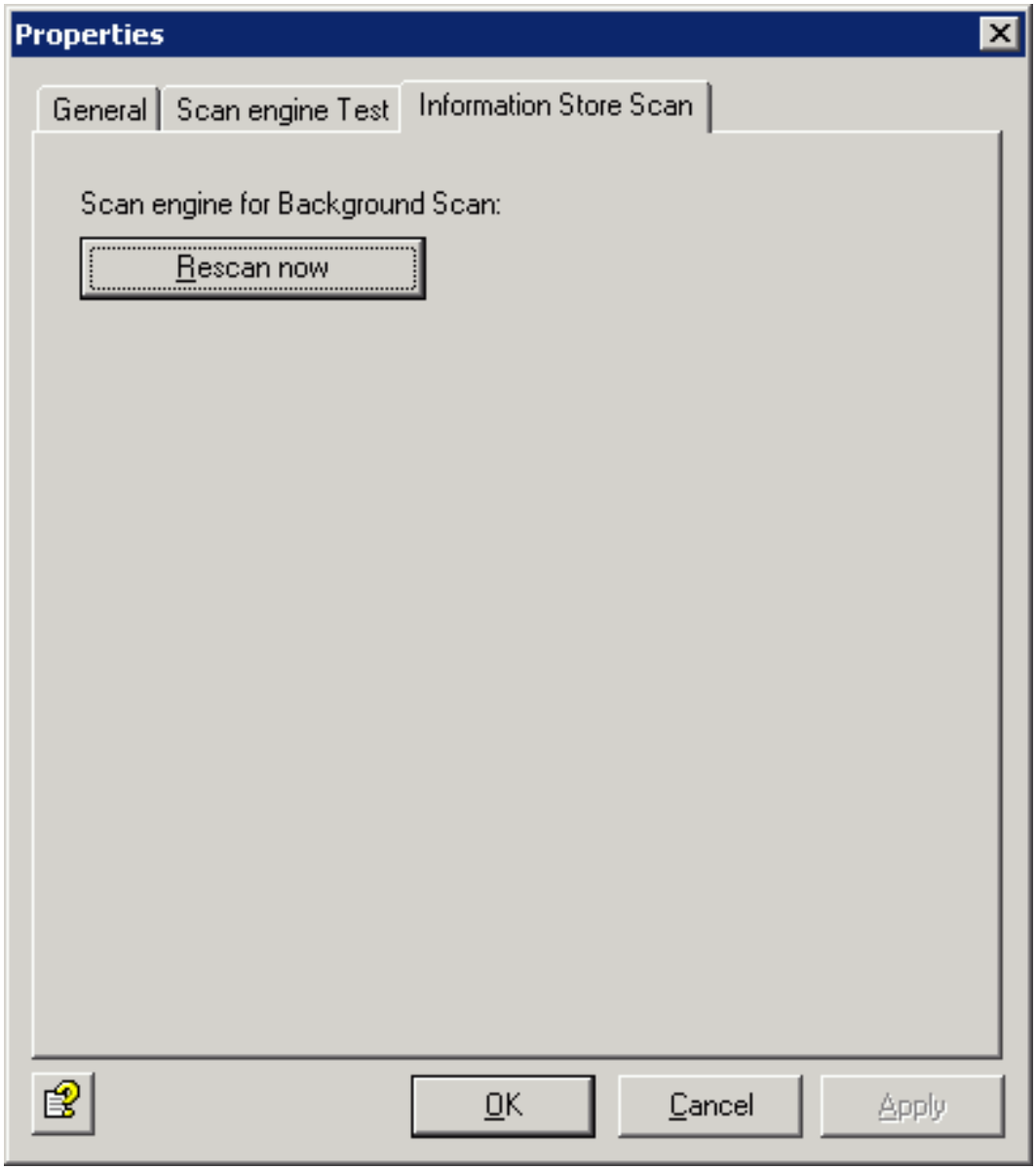
Under **AntiVir Monitor - Servers - <servername> - Server Status** you can see the current status of the Information Store scan and the option for a manual restart.

The **General** tab shows information about Server, Configuration, License and IS (Information Store) Scan:



- The status of the scanner DLL for the Information Store scan. When the DLL indicates **Loaded**, the Information Store scan is enabled.
- The Information Store scan version. This number is incremented with every restart.
- The date of the last version update and the time and date of the last restart.

Under the **Information Store Scan** tab, you can restart background scanning:



When scanning is restarted, all elements in the Information Store are checked one more time. This applies to all three scan modes. If you have enabled background scanning, this scan may take a long time and use a lot of processor capacity. It is therefore advisable to restart scanning during periods of low system usage.

4.4 File Restrictions for Attachments

Files can be restricted according to their type and size: you can deny specific file types and you can specify maximum message and attachment sizes. Both the size and the type of attachments can also be checked with a single job.

4.4.1 By Type

AntiVir must be able to identify files according to their type. This is done by way of file fingerprints, which contain a binary file pattern (for example for *.exe files) and/or the file extension (for example for *.vbs files).

The result of this scan is compared with the denied/ allowed fingerprints under **Fingerprint conditions** (set in the job properties) and blocked or delivered accordingly. For denied files, the job actions are performed, for instance for a mail with a denied attachment:

- The denied attachment is copied to the Quarantine folder.
- The message text is delivered to the recipient.
- Notifications are sent to the Administrator and the sender.

An **AntiVir Attachment Filtering** job can perform the following actions:

- Place the entire e-mail in Quarantine
- Remove affected attachments from the message
- Delete the affected message without delivering it
- Add email sender or recipients to the userlist
- Add a subject extension
- Notify the Administrator
- Notify the sender
- Notify the recipient
- Add label
- Notify other user-defined recipients
- Start external program
- Add Avira tag and value
- Add header field and value
- Redirect mail

4.4.2 By Message Size

E-mails can be scanned and denied according to their total size. The e-mail size limit is specified under the **Email Size** tab.

An **AntiVir Email Size Filtering** job can perform the following actions:

- Place the entire e-mail in Quarantine
- Add label
- Delete the affected message without delivering it
- Add email sender or recipients to userlist
- Notify Administrator, sender, recipient
- Notify other user-defined recipients
- Start external program
- Add Avira tag and value
- Add header field and value
- Redirect mail

4.4.3 By Type and/or Attachment Size

Attachments can be checked for size and messages delivered or denied accordingly. The maximum attachment size is specified on the **Fingerprint/Size** tab. This job can check and deny attachment types while at the same time filtering by attachment size.

AntiVir Attachment/Size Filtering jobs can perform the same actions as attachment filtering jobs.

4.4.4 Configuring Fingerprints

Fingerprints consist of a name pattern and/or a binary pattern.

- Filename pattern: used to define file types by filenames and file extensions (*.exe, etc.)
- Binary pattern: used to define file types using unique binary file information.

Malicious users can manipulate filenames by simply changing the extension to a different file type. To prevent file type filtering being fooled by this type of manipulation, you can use the binary pattern which uniquely identifies file formats. The binary pattern is therefore the most reliable method for identifying file types.

Filename patterns, however, can be used to quickly react to new virus attacks:

As soon as the extension of the file containing a virus is known (for example Nimda Virus = readme.exe), a virus infection can be prevented even before a virus pattern update is available from the publisher of your antivirus application. A new fingerprint with the filename pattern is simply created to identify the virus.

You can also block individual files:

If your company employs custom software that uses its own file formats, you can also create fingerprints for these files, which you can use, for example, to prevent files of this type being sent as e-mail attachments to recipients outside the company.

Sorting and grouping fingerprints

You can sort fingerprints and group them into logical categories. Fingerprint categories are listed alphabetically.

1. Go to **Basic Configuration - Utility Settings - Fingerprints** to view all available categories in the right pane.
2. Doble-click a category to open it.

   The individual fingerprints appear in the right pane.

3. You can drag individual fingerprints from the right pane into a different category in the left pane.
4. To view the **Properties** of a fingerprint in the right pane, double-click or right-click the fingerprint.

Note: *To copy fingerprints from the* ***All Fingerprints*** *category, drag them to the desired category. When you drag fingerprints from any of the other categories, they are* ***moved!*** *To copy from other categories, hold the Ctrl key while dragging. A plus symbol then appears in the cursor.*
Attention: *When you delete a fingerprint from any category with the Del key, it is permanently deleted and can not be restored. To remove a fingerprint from a category without permanently deleting it, right-click it and select* ***All Tasks - Remove fingerprint(s) from this category****. Make sure that the fingerprints you want to delete or remove are no longer used by an Avira AntiVir Exchange job.*

To create a new fingerprint category, click on Fingerprints in the left pane, right-click and select **New - Fingerprint Category**. For a new fingerprint, right-click the category and select **New - Fingerprint**.

The **Jobs** tab in the fingerprint properties shows the list with the jobs that use the fingerprint.

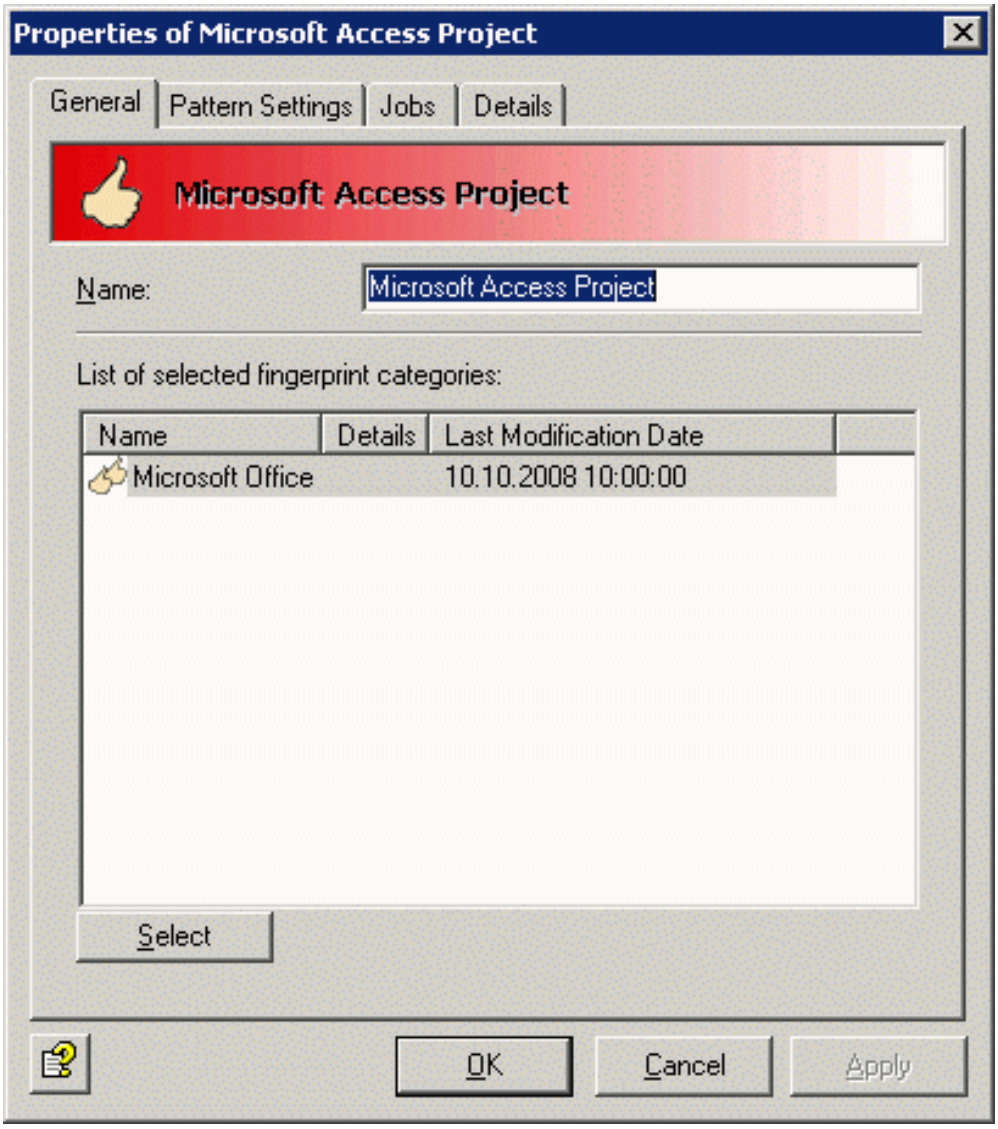
Creating Fingerprints with Name Patterns

If a file's binary pattern is not known, it can be identified quickly using a name pattern.

1. Double-click a fingerprint to open the **Properties**

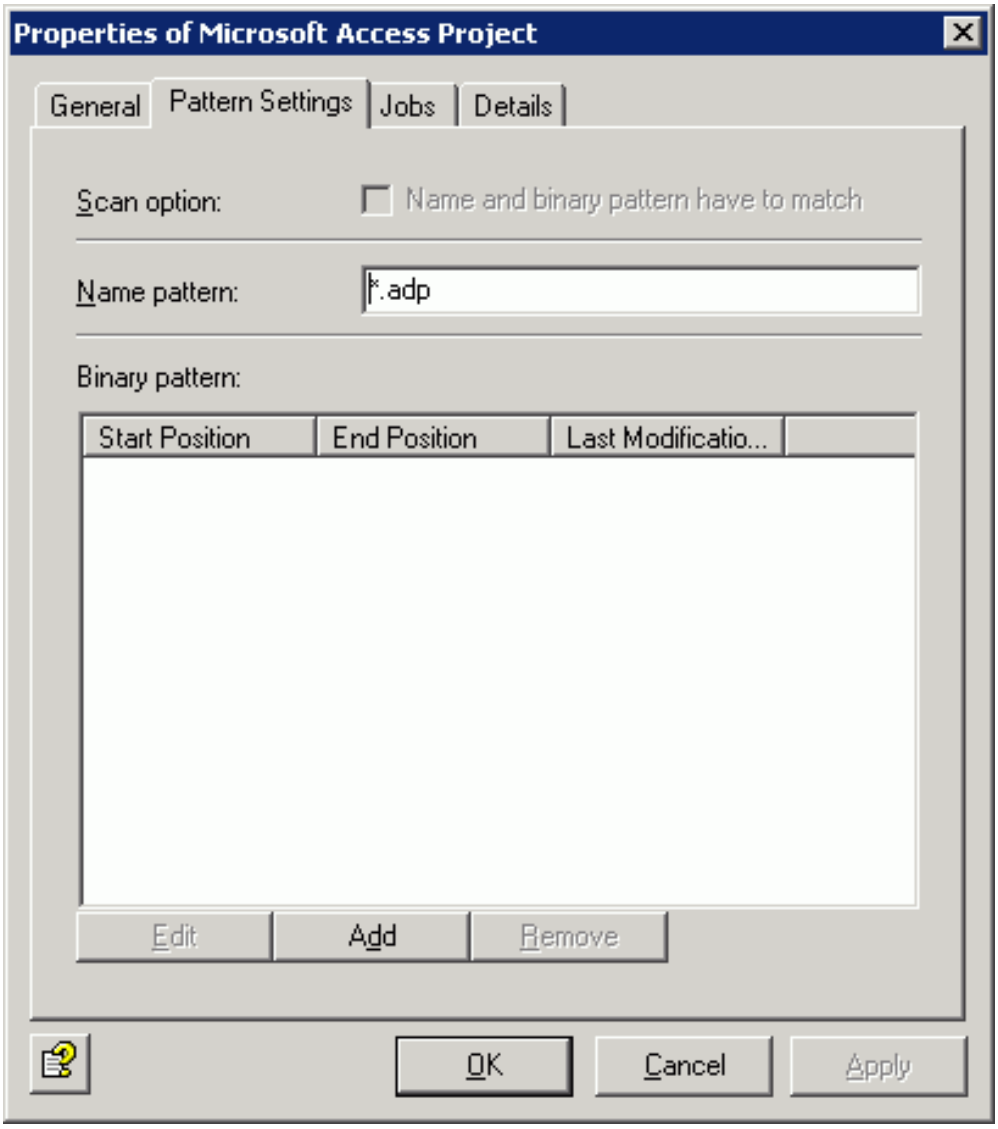
   The **General** tab (refer to Configuring Fingerprints) shows the fingerprint's name

and categories (with a Microsoft fingerprint in the example below):



The fingerprint is called **Microsoft Access Project** and belongs to the **Microsoft Office** category.

2. Select the **Pattern Settings** tab.



3. In the **Name pattern** field, enter the file extension for this name pattern.

Note: *You can define several filename patterns for each fingerprint. Multiple entries must be separated with a semicolon (;). You can use the "*" wildcard for multiple characters, for instance to define a fingerprint with the filename pattern "*.vbs". You can also specify complete filenames in this field. If you enter, for instance, "Att01.cdf" here, the created fingerprint, when specified in a job, denies all files with that name.*
Note: *If you have selected the option* ***Name and binary pattern have to match****, both the filename pattern (file extension) and the binary pattern of the checked file must correspond with the data in the fingerprint properties. Make sure that you have specified this information. If you have not selected this option, but both patterns have been specified in the fingerprint properties, only one of the patterns must match to identify the file format. For further information on entering name and binary patterns, refer to Selecting Fingerprints .*

Creating Binary Patterns for Fingerprints

Description

Binary patterns contain the following information:

- Start position
- End position
- Hexadecimal values

1. **Start position**: The position within a file from which a pattern search is performed.

   The following values are possible:

1	Start at the first byte of the file
1, 2, ...	Start at the first byte, second byte, etc. of the file
-1 ...	Start at the last byte of the file
-6 ...	Start at the sixth byte from the end of the file

2. **End position**: The position within a file up to which the pattern search is performed.

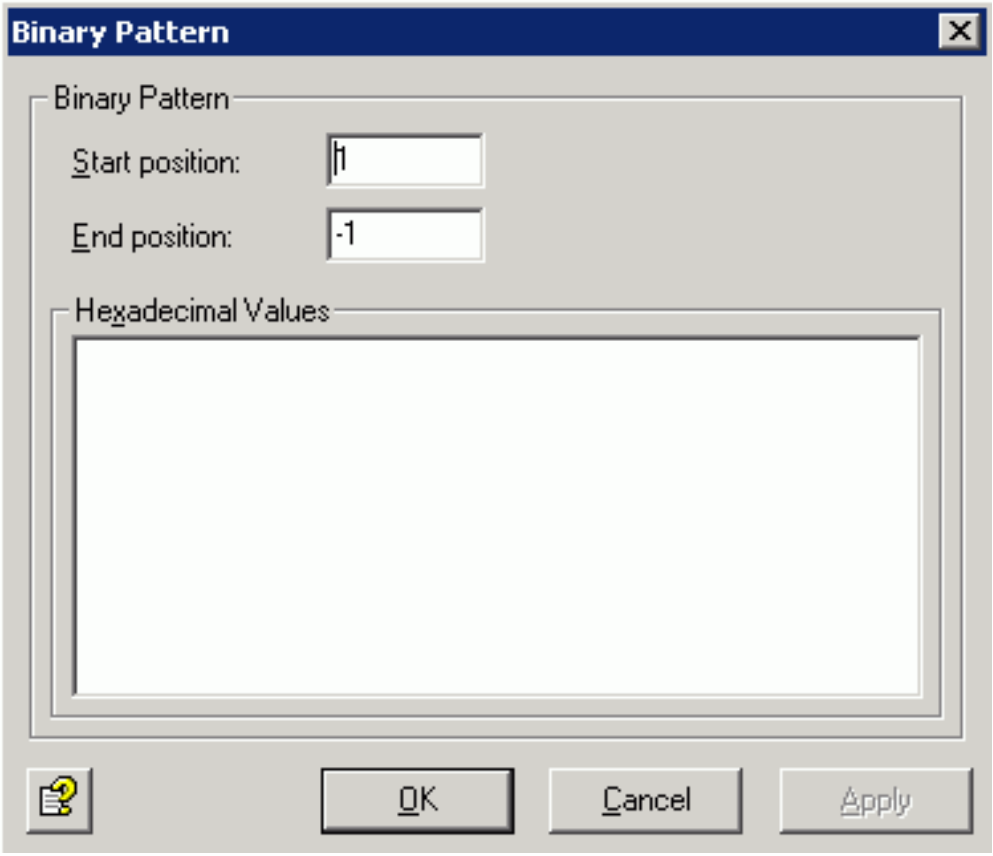
   The following values are possible:

-1	Search to the end of the file
1, 2 ...end	Search up to byte 1, byte 2, etc. of the file
-11 ...	Search to the eleventh byte from the end of the file

3. **Hexadecimal values**: The pattern to be searched for between the start and end positions.

   Fingerprints can consist of several binary patterns.

1. Go to the fingerprint **Properties** (refer to Configuring Fingerprints) and select the **Pattern Settings** tab.
2. Click **Add**.
3. Enter the **Start position**, the **End position** and the **Hexadecimal** search value.



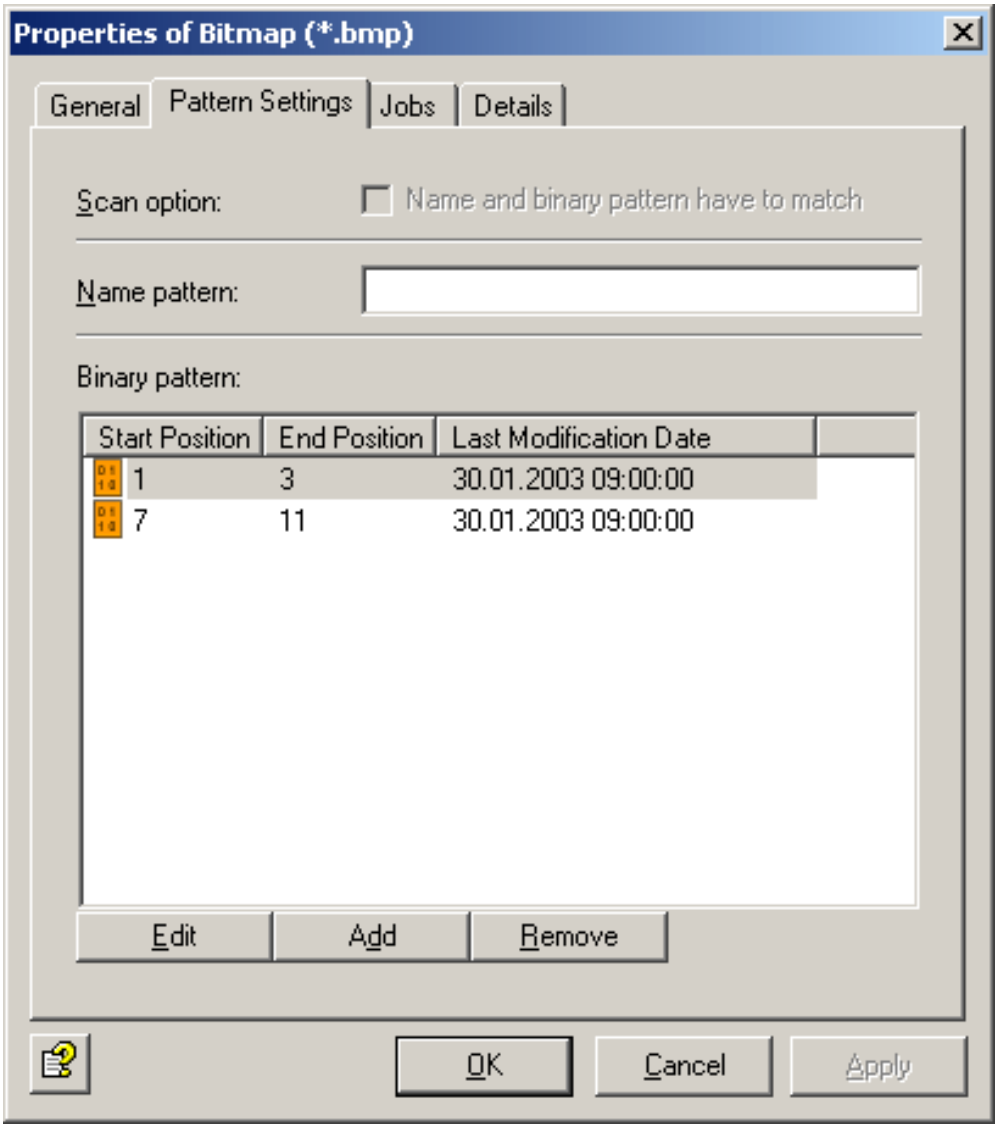
The start position is the point in the file from which the specified binary pattern will be searched for. The position of the first byte in the file, i.e. the beginning of the file, is offset 1. The second byte then has an offset of 2, etc. The end position is the offset up to which the pattern is searched for.

If the number in one or both of these fields is prefixed with a minus sign (“-”), the bytes are counted in reverse. The entry -1, for example, is the last byte of the file. -2 would then be the last but one byte, etc. The file size is irrelevant for this purpose. A start position of 1 and an end position of -1 means that the entire file will be searched for the specified pattern. You can also enter two negative values for example -6 as start position and -1 as end position. The search is then performed from the last byte to the sixth from last byte, regardless of the byte size of the file.

A positive start position and a negative end position are always possible, for example 11 as start position (the eleventh byte) and -10 as end position (the tenth byte from the end). You can not enter a negative start position and a positive end position.

Example: Windows/OS2 Bitmap files (*.bmp)

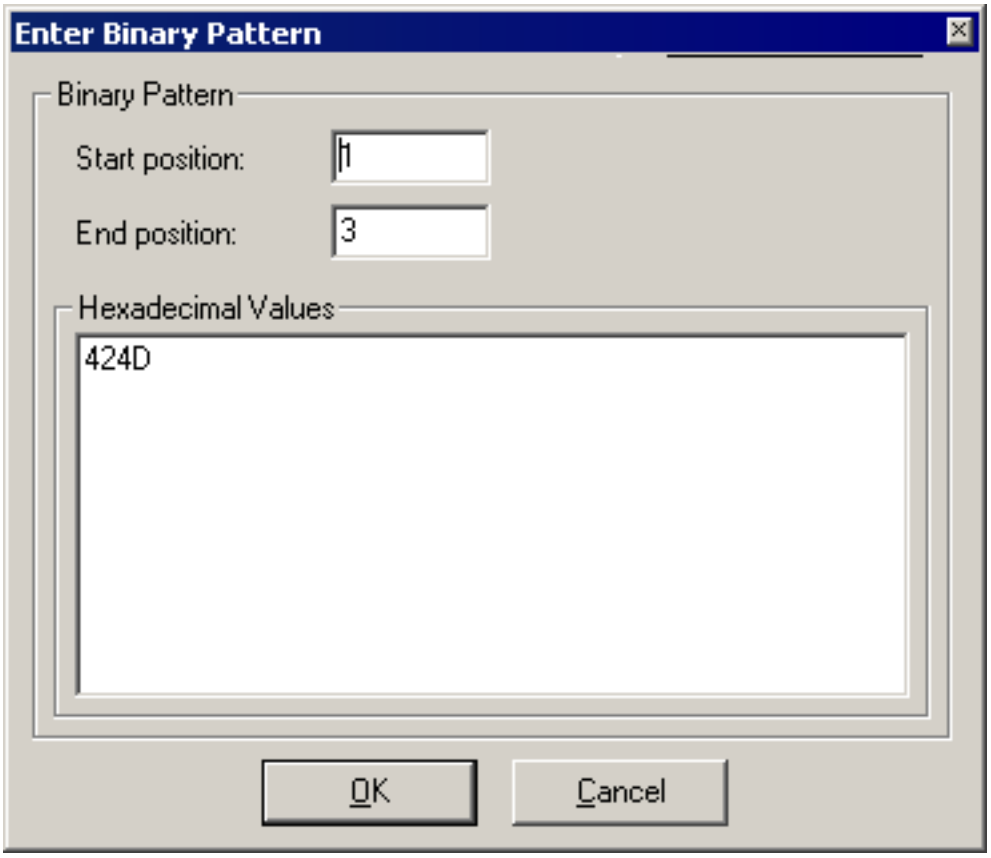
When you open the pattern settings for a bitmap file, the following dialog appears:



For details on the **Check Binary and Name Pattern** option, refer to Configuring Fingerprints .

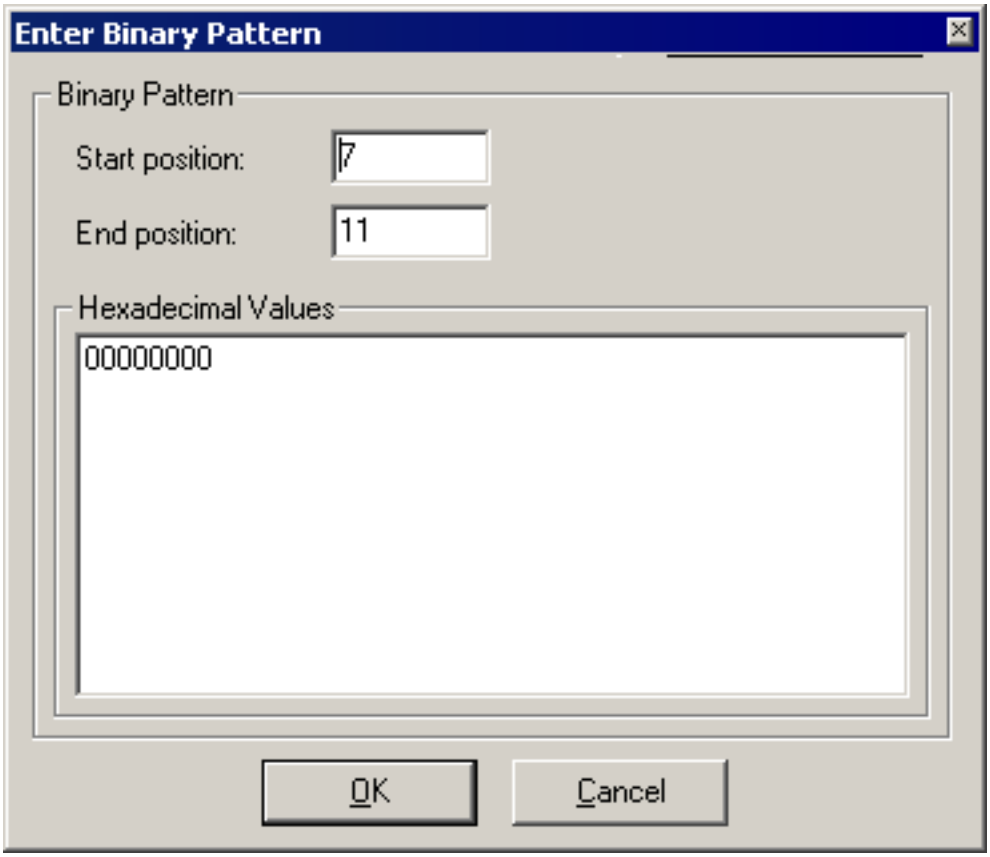
4. Now click **Edit** to open the first entry.

   The following dialog appears:



The start position is “1”, the end position “3”. This means that the file is searched for the binary pattern “**42 4D**” between the first and the third byte, i.e. between offset 1 and offset 3. The binary pattern is entered as a hexadecimal number in the lower field. The pattern in this example corresponds to the letters “BM”. This is part of the ID of a Windows/OS2 bitmap file. This is still not a complete pattern.

5. To complete the binary pattern for a bitmap file, you must add one more entry, which looks like this:



Here, a search is performed for the pattern “00000000” between offsets 7 and 11.

Only when both binary patterns have been found in a file, does the file match the pattern and can be identified as a bitmap.

6. For each additional search pattern, click **Add**.

Note: *If you want to identify fingerprint binary patterns that are not included in the supplied list of file patterns, please contact the publisher of the software to which the file type applies, e.g. Adobe for Acrobat (*.pdf) files or contact our Support.*

Further Fingerprint Examples

Example of a simple fingerprint: ZIP file

Start	End	Hex value
1	4	504B0304

Example of a more complex fingerprint: Windows Meta File

Start	End	Hex value
1	13	576F72642E446F63756D656E74
1	-1	57006F007200640044006F0063 0075006D0065006E0074
1	10	D0CF11E0A1B11AE10000

4.4.5 Denying File Attachments by Type - Example

Under **Policy Configuration - Job Templates**, you will find various jobs for blocking different file formats.

- **Block all archives except ZIP-files**

  Blocks all compressed formats except ZIP files

- **Block suspicious attachments**

  Blocks known malicious attachments such as Nimda.

- **Block images**

  Blocks image formats

- **Block video files**

  Blocks video formats

- **Block sound files**

  Blocks sound formats

- **Block executable files**

  Blocks exe, com, files, etc.

We will use the **Block video files** job as an example. Drag this job to the **Mail Transport Jobs** folder and open it there with a double-click.

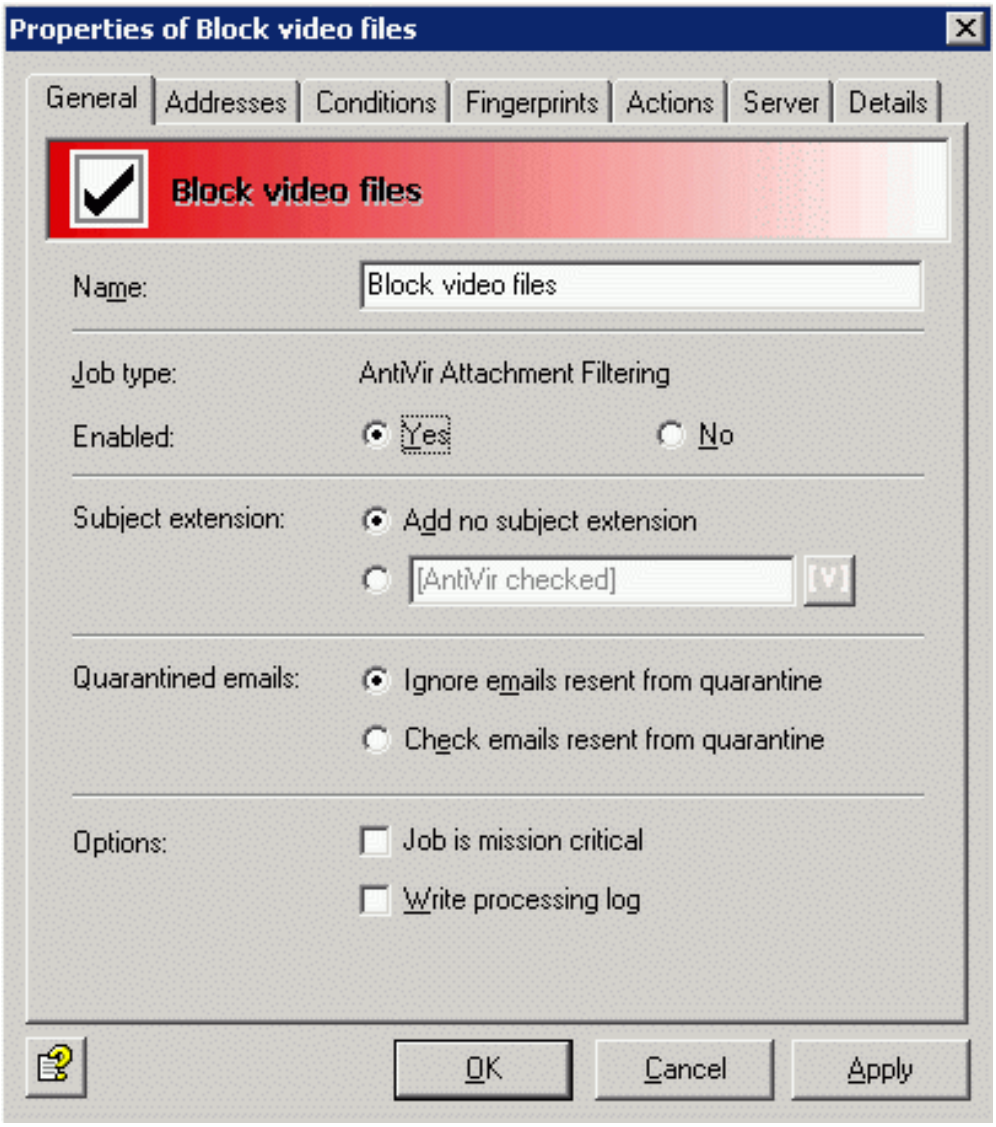
General Settings

1. Under the **General** tab, enter a name for the job.

   An active (enabled) job has a checkmark in the the job symbol.

2. Set the job to **Enabled: Yes**.
3. Save your settings with **Apply** and close the job.

   The job is enabled.



By default, the **Subject extension** is pre-set to **AntiVir checked**. If enabled, this text is added to the subject of each mail checked by the job.

This job does not process mails that are being resent from **Quarantine (AntiVir Monitor - <select quarantine item> - All Tasks - Resend quarantine item**), even if the **Resubmit the email to all AntiVir jobs** has been enabled. The **Ignore emails resent from quarantine** option means that this job is systematically skipped when a mail is resent from Quarantine.

Setting up Address Conditions

1. Under the **Addresses** tab, specify the senders or recipients to which this job is to apply.

   You can select addresses from existing lists or define others.

2. Click on the **Save** button .

   Save the configuration of the AntiVir Exchange Management Console each time

you have modified the settings.

The configuration is saved in the `ConfigData.xml` file located in the `Avira\AntiVir Exchange\Config\` folder.

Pending changes are indicated by an asterisk (*) next to the top node.

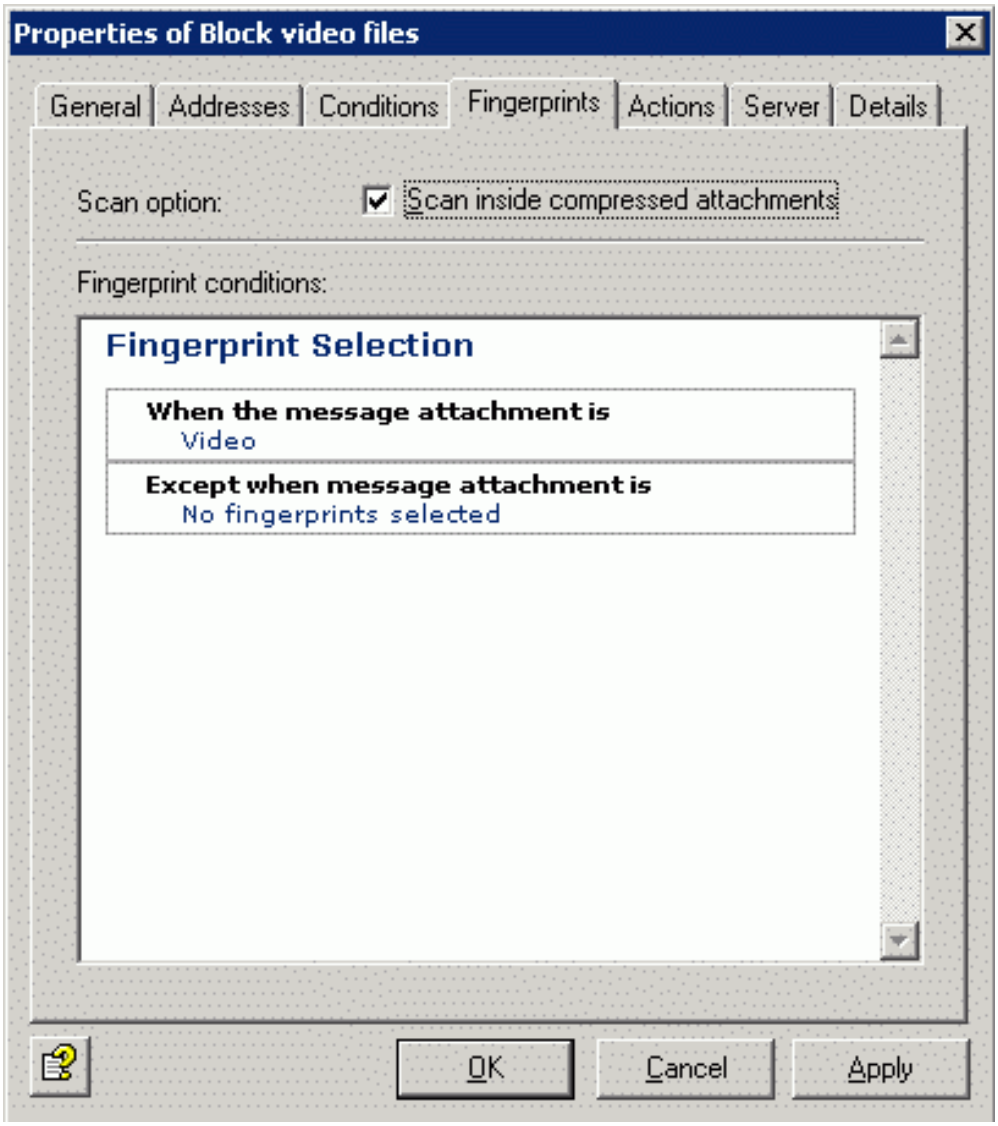
Setting up Content Conditions

Under the **Conditions** tab you can set the requirements as to which mails or documents a job is to be run for.

Note: *The content conditions and the address conditions set in the* ***Addresses*** *tab must simultaneously come true, for a job to be run (logical AND).*

Selecting Fingerprints

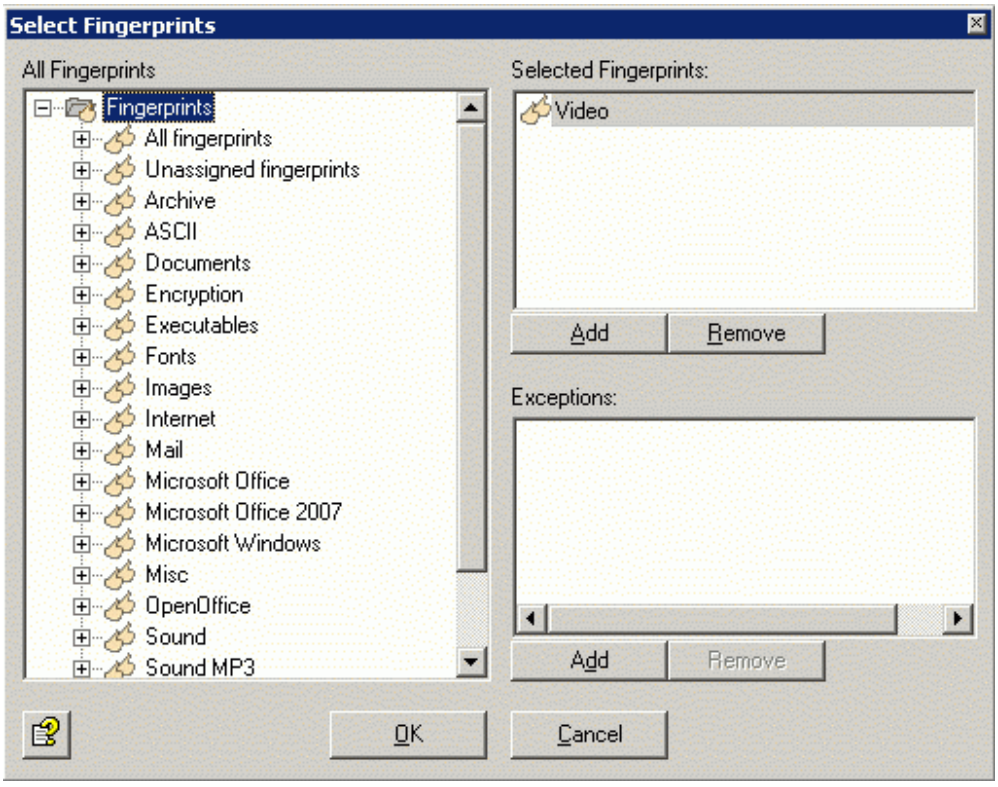
1. Under the **Fingerprints** tab, select the denied fingerprints:



Scan inside compressed attachments means that the internal unpacker opens archives and checks the files it contains for the fingerprints specified. If this option is disabled, only the archive is checked and identified as compressed format.

2. Fingerprint conditions: Click **Video** or **No fingerprints selected** to select a fingerprint category or an individual fingerprint from the list.

   The following view appears:

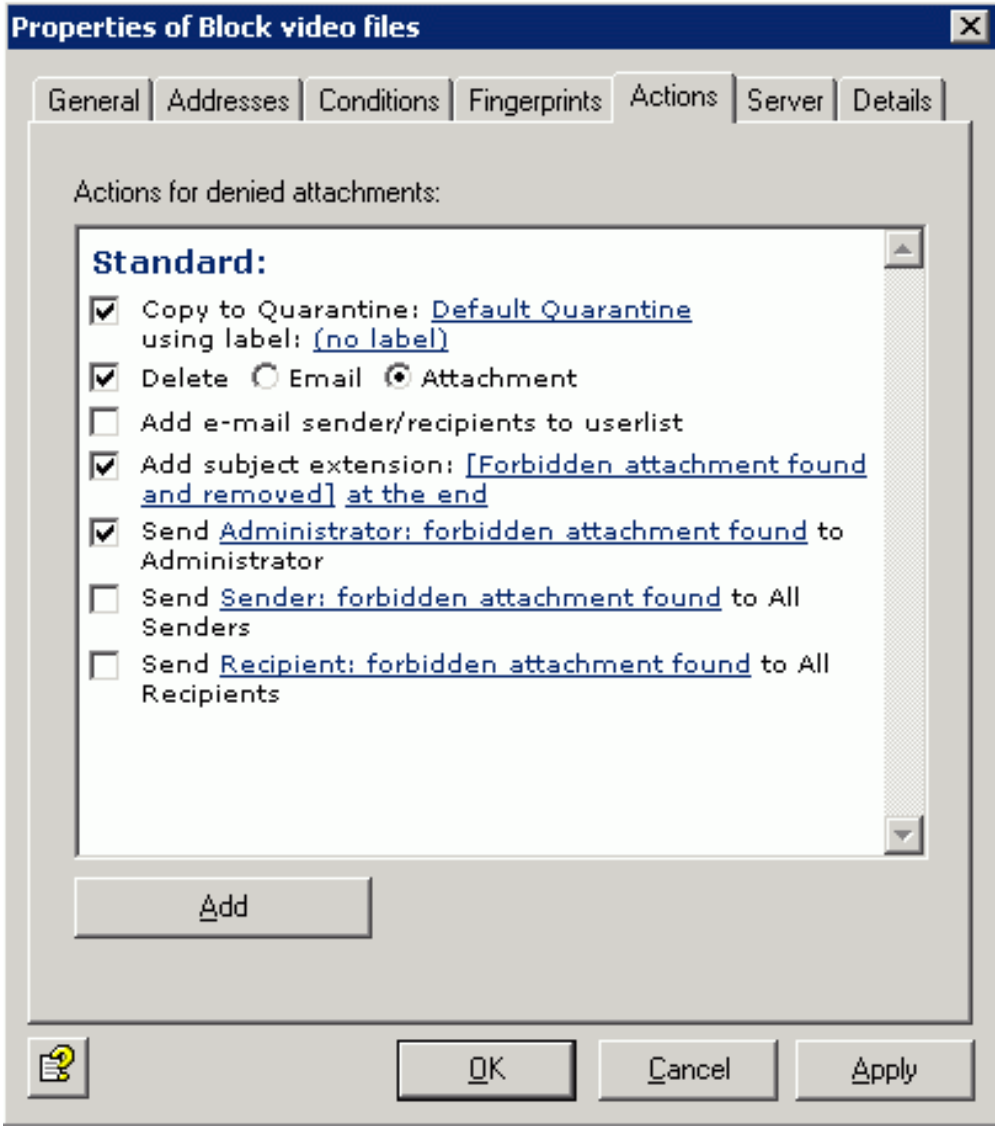


3. Double-click the category in the left pane or click the **+** sign to open it, then press the **Add** or **Remove** buttons, to assign entire categories or individual fingerprints to the list of denied and/or allowed fingerprints.

Tip: *You can enter a category such as "Video" under* ***Selected Fingerprints*** *and define one or more fingerprints from that category as exception under* ***Exceptions****. To keep a clear overview, do not use the same job for too many categories.*

Defining Actions

1. Under the **Actions** tab, specify the actions to be performed **when the job finds an attachment with a denied fingerprint.**



In this example, a copy of the e-mail is placed in Quarantine and the infected attachments are deleted. The message is delivered to its recipient, but the denied attachments are removed. A notification about the denied fingerprint is sent to the Administrator. You can select this notification from the list menu of available notification templates, which you can format using the HTML toolbar or by directly entering appropriate HTML code.

2. To define further actions, press the **Add** button.

4.4.6 Limiting Message Size - Example

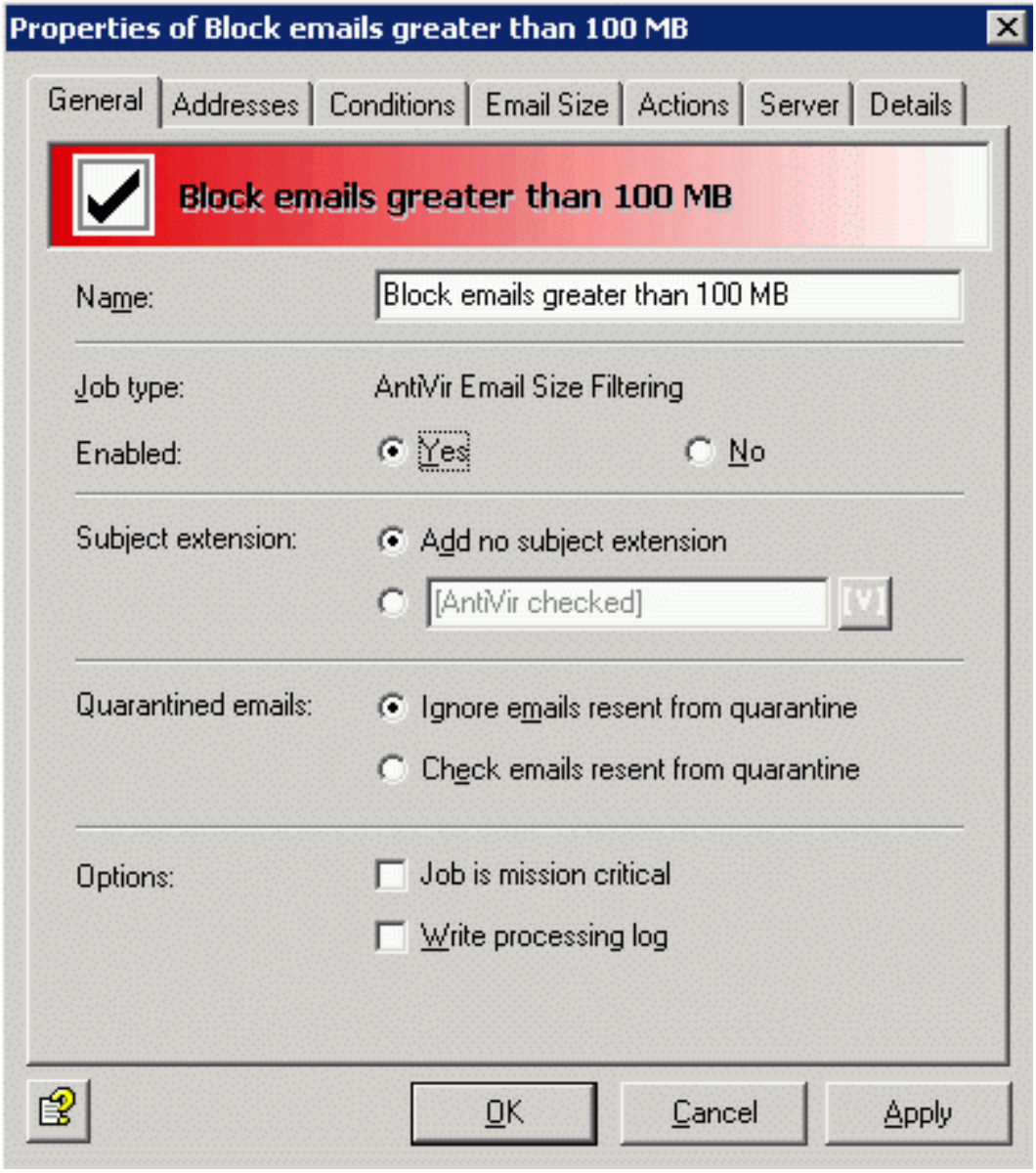
Under **Policy Configuration - Job Templates** you will find the **Block emails greater than 100 MB** job.

Tip: *The message size limit applies to the e-mail as a whole, including subject, text body, header and attachments.*

Drag this job to the **Mail Transport Jobs** folder and open it there with a double-click.

General Settings

Under the **General** tab, enter a name for the job. An active (enabled) job has a checkmark in the job symbol. Set the job to **Enabled: Yes**. Once you have saved your settings with **Apply** and closed the job, the job is active.



By default, the **Subject extension** is pre-set to **AntiVir checked**. If enabled, this text is added to the subject of each mail checked by the job.

This job does not process mails that are being resent from **Quarantine (AntiVir Monitor - <select quarantined email> - All Tasks - Resend quarantine item)**, even if the **Resubmit the email to all AntiVir jobs** has been enabled. The **Ignore emails resent from quarantine** option means that this job is systematically skipped when a mail is resent from Quarantine.

Setting up Address Conditions

Under the **Addresses** tab, specify the senders or recipients to which this job is to apply.

You can select addresses from existing lists or from your own ones.

For details on how to make the best use of address lists and details, refer to the description under Address Lists .

Setting up Content Conditions

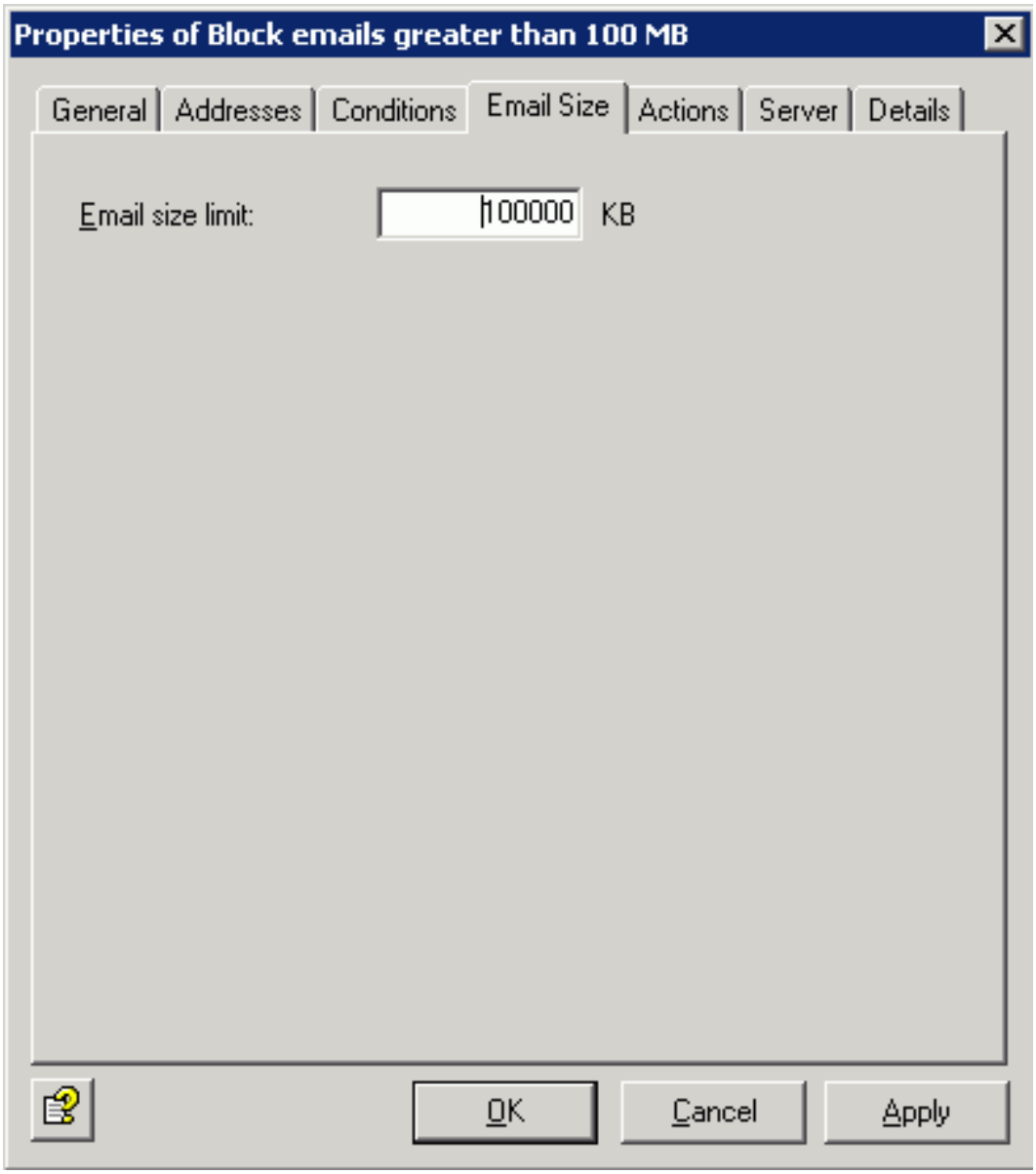
Under the **Conditions** tab you can set the requirements as to which mails or documents a job is to be run for.

For the use and settings of conditions refer to Conditions .

Note: *The content conditions and the address conditions set in the* ***Addresses*** *tab must simultaneously come true, for a job to be run (logical AND).*

Specifying Message Size

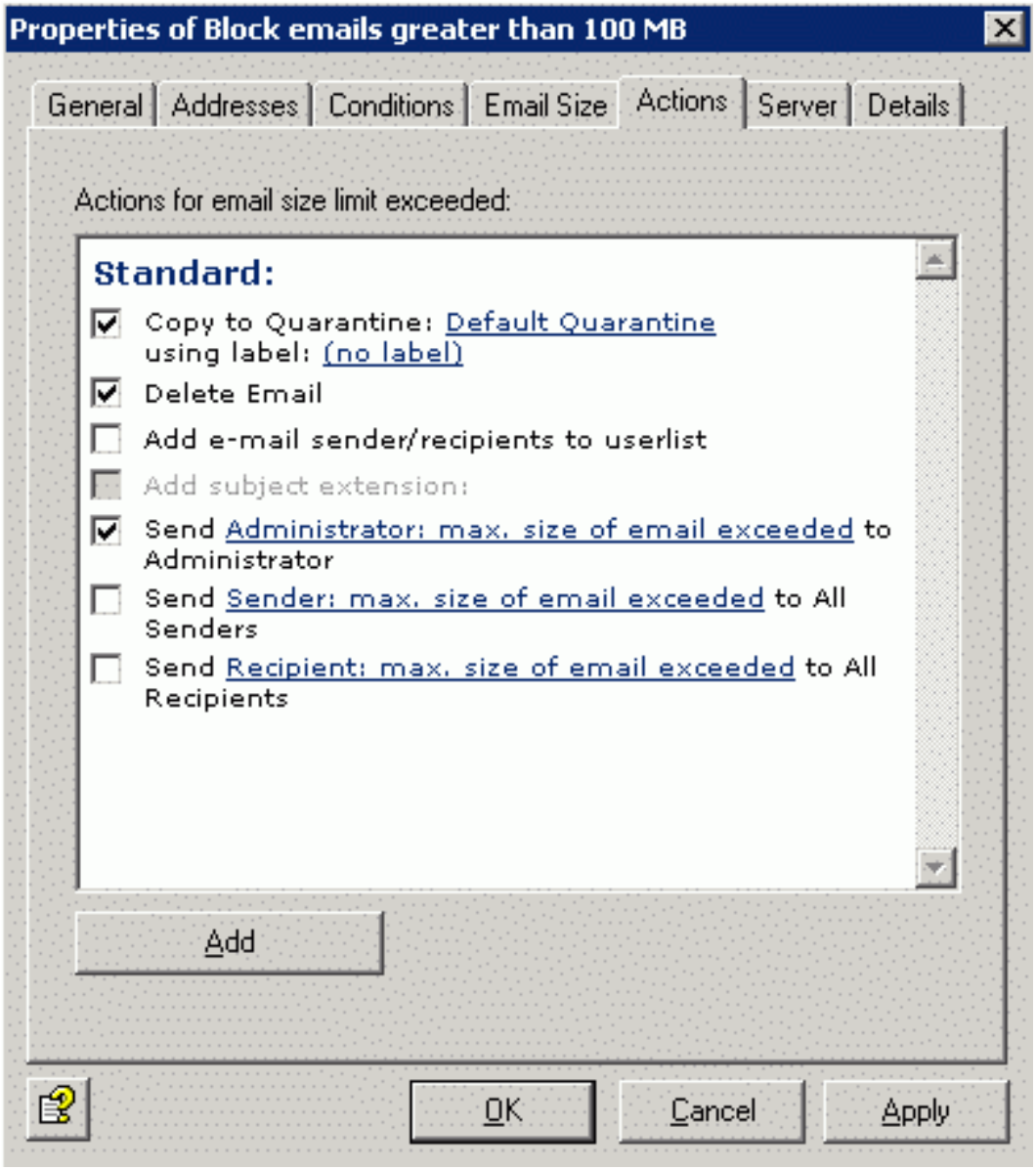
Under the **Email Size** tab, enter the e-mail size limit in kilobytes:



With the setting above, the maximum allowed size of each incoming and outgoing e-mail is 100.000 kilobytes.

Defining Actions

Under the **Actions** tab, specify the actions to be taken when the job finds an e-mail that exceeds the maximum size.



In this example, a copy of the message is placed in Quarantine and the message is deleted without being delivered to its recipient. A notification about the excessive message size is sent to the Administrator. You can select this notification from the list menu of available notification templates, which you can format using the HTML toolbar or by entering appropriate HTML code yourself.

To define further actions, click the **Add** button.

For a description of the procedure, refer to the description in the AntiVir chapter under

Enabling Virus Scanning - Example, "Defining Actions" .

Selecting Servers / Job Details

To select servers and specify job details proceed as described under Selecting Servers and Entering Job Details .

Save the configuration of the AntiVir Exchange Management Console each time you have modified the settings. Click on the **Save** button . The configuration is saved in the `ConfigData.xml` file located in the `Avira\AntiVir Exchange\Config\` folder. Pending changes are indicated by an asterisk (*) next to the top node.

4.4.7 Denying Attachment Types and Sizes - Example

Under **Policy Configuration - Job Templates** you will find a number of jobs for blocking various file formats and sizes:

- **Block office files > 10 MB**

  Microsoft Office files exceeding 10 MB

- **Block sound files > 5 MB**

  Sound files exceeding 5 MB

- **Block video files > 5 MB**

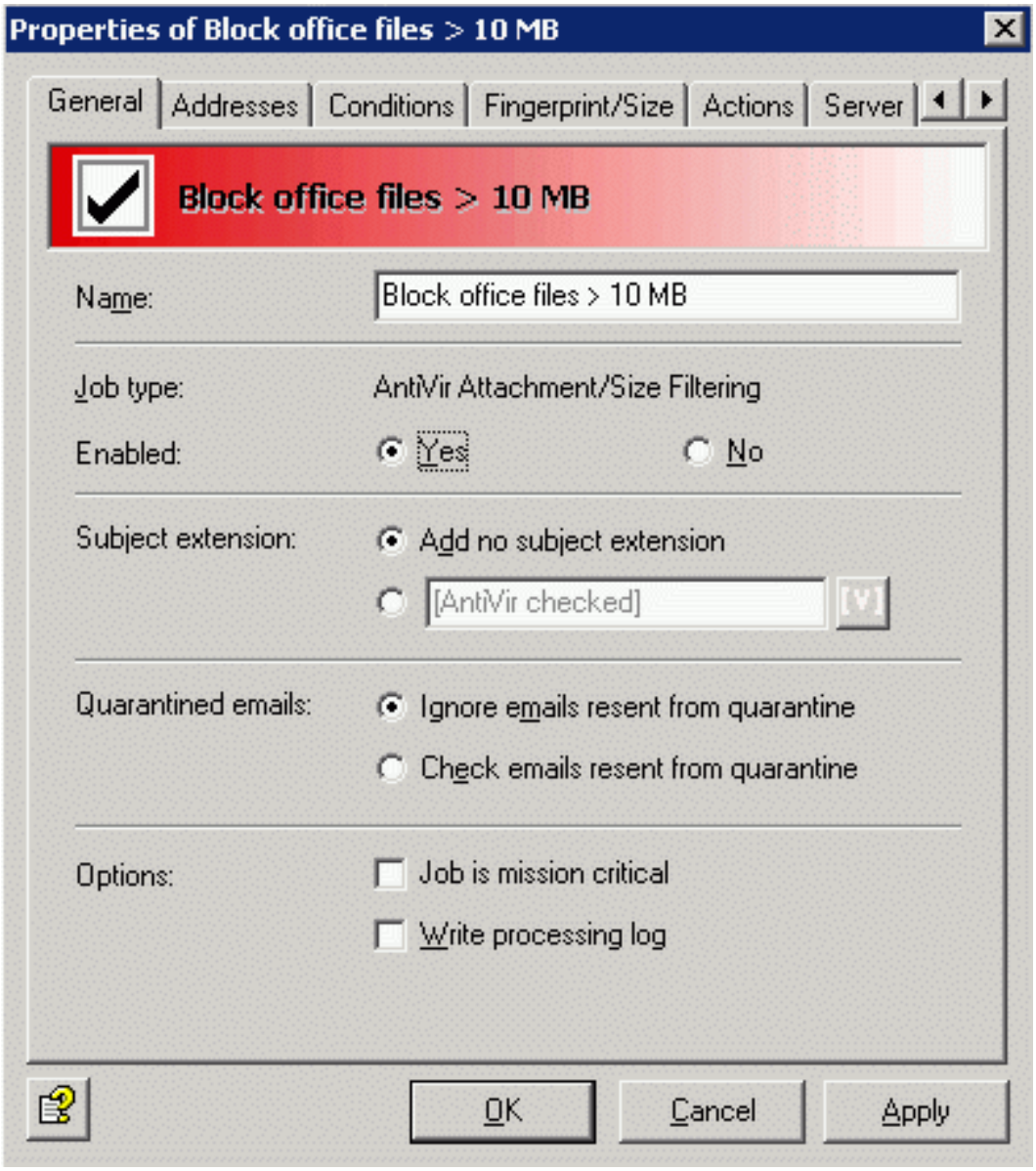
  Video files exceeding 5 MB

Tip: *Unlike checking the e-mail size, checking the format and the size of attachments applies to attachments only. Neither the subject nor the message body nor the e-mail header are taken into account.*

We will use the **Block office files > 10 MB** job as an example. Drag this job to the **Mail Transport Jobs** folder and open it there with a double-click.

General Settings

Under the **General** tab, enter a name for the job. An active job has a checkmark in the job symbol. Set the job to **Enabled: Yes**. Once you have saved your settings with **Apply** and closed the job, the job is active.



By default, the **Subject extension** is pre-set to **AntiVir checked**. If enabled, this text is added to the subject of each mail checked by the job.

This job does not process mails that are being resent from **Quarantine (AntiVir Monitor - <select quarantined email> - All Tasks - Resend quarantine item)**, even if the **Resubmit the email to all AntiVir jobs** has been enabled. The **Ignore emails resent from quarantine** option means that this job is systematically skipped when a mail is resent from Quarantine.

For further information on sending quarantined mail refer to Sending From Quarantine . For details on the **Mission Critical** option refer to This job is mission-critical in the section "AntiVir".

Setting up Address Conditions

Under the **Addresses** tab, specify the senders or recipients to which this job is to apply. You can select addresses from existing lists or from your own ones.

For details on how to make the best use of address lists and details, refer to the description under Address Lists .

Setting up Content Conditions

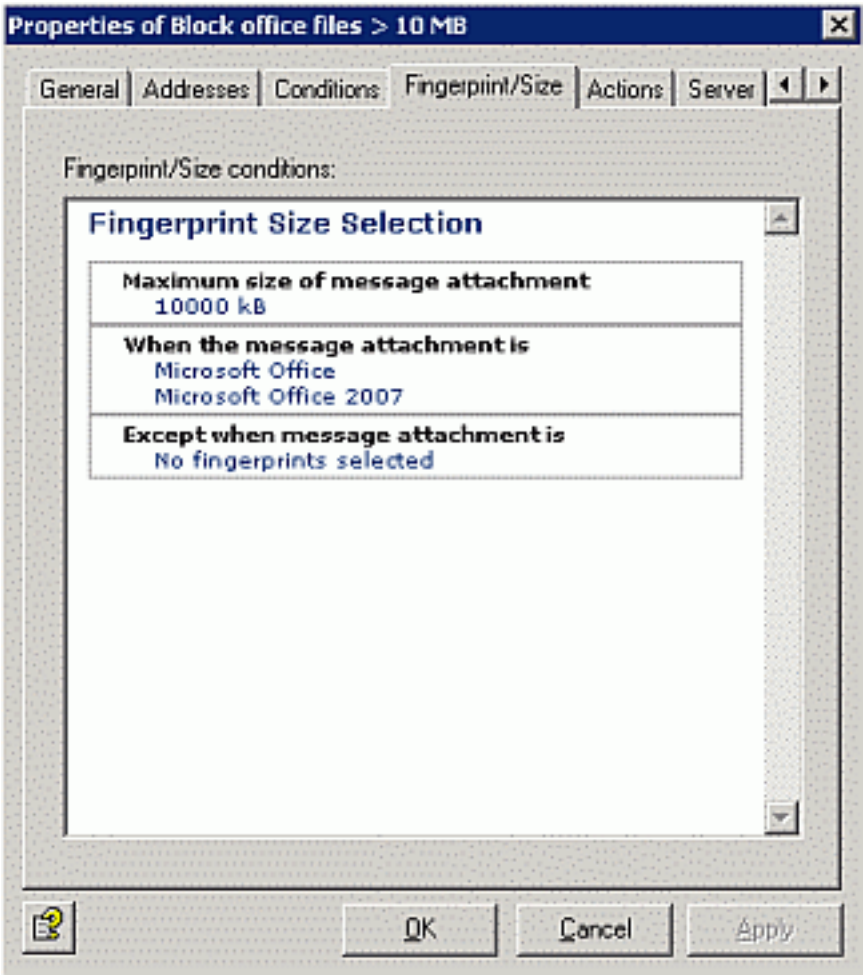
Under the **Conditions** tab you can set the requirements as to which mails or documents a job is to be run for.

For the use and settings of conditions refer to Conditions .

Note: *The content conditions and the address conditions set in the* ***Addresses*** *tab must simultaneously come true, for a job to be run (logical AND).*

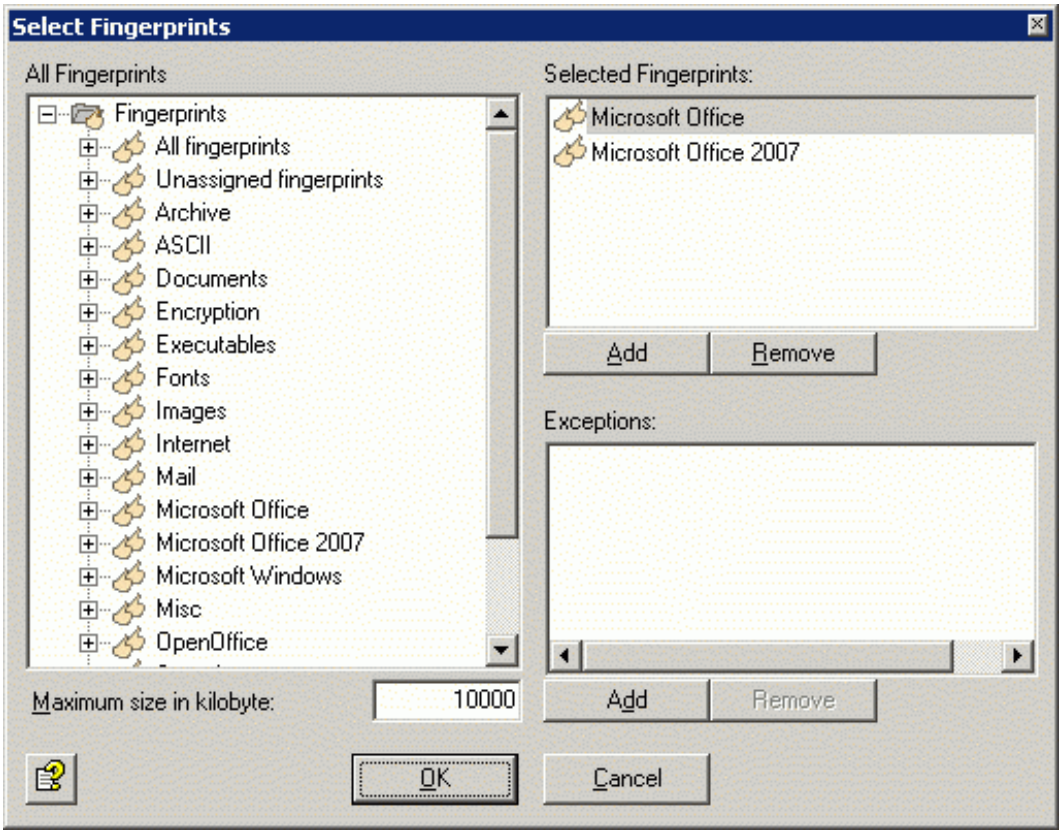
Specifying Fingerprint and Size

Under the `Fingerprint/Size` tab, enter the maximum permissible e-mail size and the fingerprint format:



Note: *Unlike for simple fingerprint checking, the* ***Scan inside compressed attachments*** *option is not available here. To limit the size of compressed files, enter their formats in this job.*

Fingerprint/Size conditions: To specify the size in kilobytes, click **10000**. To select a fingerprint category, an individual fingerprint or the maximum size from the list of fingerprints, click on **Microsoft Office**. The following view is displayed:



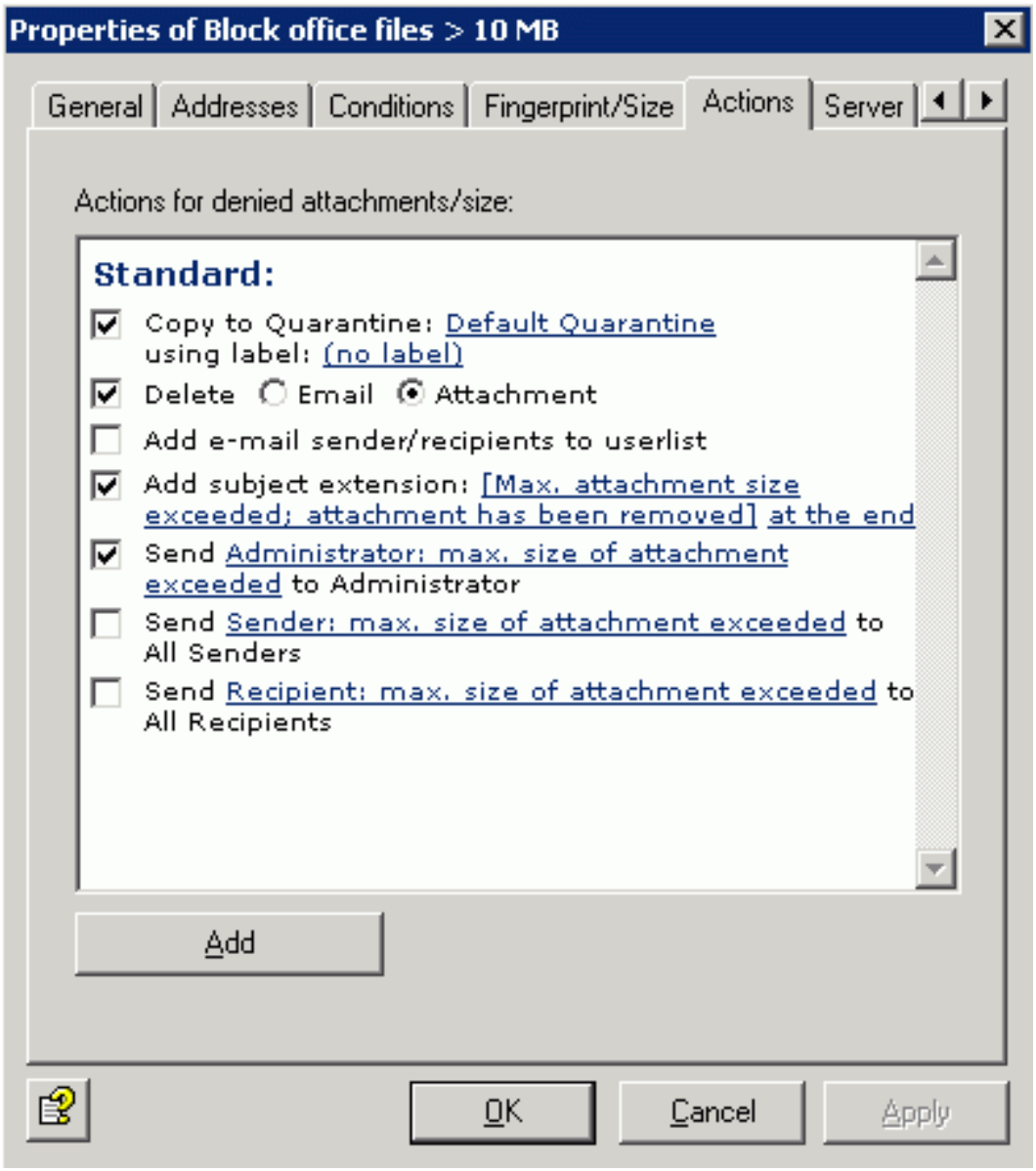
With the **Add** and **Remove** buttons, you can assign entire categories or individual fingerprints to the list of denied and/or allowed fingerprints. To do so, double-click the category in the left pane or click the **+** sign to open it.

Tip: *You can enter a category such as "Microsoft Office" under* ***Selected Fingerprints*** *and define one or more fingerprints from that category as exception under* ***Exceptions****. To keep a clear overview, do not use the same job for too many categories.*

For further information on fingerprints and on entering name and binary patterns, refer to Configuring Fingerprints .

Defining Actions

Under the **Actions** tab, specify the actions to be taken **when the job finds an e-mail that was denied by an attachment/size job**.


Properties of Block office files > 10 MB
General
Addresses
Conditions
Fingerprint/Size
Actions
Server
Actions for denied attachments/size:
Standard:
Copy to Quarantine: Default Quarantine
using label: (no label)
Delete Email Attachment
Add e-mail sender/recipients to userlist
Add subject extension: [Max. attachment size exceeded; attachment has been removed] at the end
Send Administrator: max. size of attachment exceeded to Administrator
Send Sender: max. size of attachment exceeded to All Senders
Send Recipient: max. size of attachment exceeded to All Recipients
Add
OK
Cancel
Apply

In this example, a copy of the message is placed in Quarantine, the infected attachments are deleted, and the message is delivered without its attachment. A notification on the restriction is sent to the Administrator. You can select this notification from the list menu of available notification templates, which you can format using the HTML toolbar or by entering appropriate HTML code yourself.

To define further actions, click the **Add** button.

For a description of the procedure, refer to the description in the AntiVir chapter under Enabling Virus Scanning - Example, "Defining Actions" .

Selecting Servers / Job Details

To select servers and specify job details proceed as described under Selecting Servers and Entering Job Details .

5 AntiVir Wall

5.1 Overview

AntiVir Wall is used to filter e-mails or attachments according to their text content, check images for offensive contents, classify e-mails according to their content, to restrict inbound or outbound e-mail addresses and to limit the number of recipients per e-mail.

Job types

- Filtering by e-mail address

  Job Type: **AntiVir Wall Email Address Filtering**

- Filtering by message or attachment content

  Job Type: **AntiVir Wall Content Filtering**

- Spam filtering

  Job Type: **AntiVir Wall Spam Filtering**

- Checking for offensive images with Xblock

  Job Type: **AntiVir Wall Xblock Image Filtering**

- Restricting the number of recipients

  Job Type: **AntiVir Wall Recipient Limit Filtering**

Note: *Create a separate job for each restriction type! Job types cannot be changed later.*

For details on setting up jobs, refer to the sample jobs, such as Blocking Senders and/or Recipients - Example .

5.2 Address Filtering

Address filtering focuses on the senders and recipients of the e-mails. You can deny specific senders, so that no mail from these addresses is delivered to your users, and you can deny specific recipients, so that none of your employees (or only selected people) can send mail to them.

The following objects can be used for address filtering:

- Mail-Enabled Active Directory user
- Mail-Enabled Active Directory groups
- Mail-Enabled Active Directory contacts
- User-definable SMTP addresses including wildcards
- [INTERNAL] – domains defined as internal in Avira AntiVir Exchange
- [EXTERNAL] – all addresses that are not [INTERN]
- “Administrator” – the e-mail addresses defined as Administrator in Avira AntiVir Exchange.

Senders and recipients are defined by the corresponding e-mails fields. A sender can be either an employee of your company sending e-mail to someone outside or someone outside sending an e-mail to an employee of your company. You can define both senders and recipients as individuals or groups.

For address filtering, you can normally use the following wildcards:

- Asterisk (*)

  The asterisk is the wildcard for one or more letters and digits. It can be used several times within a word or expression.

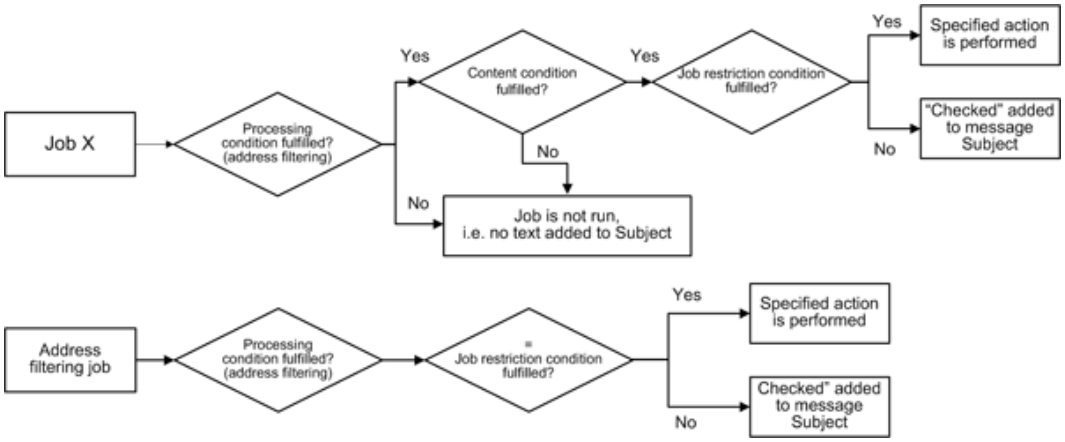
- Question mark (?)

  The question mark represents a single character. It can also be used several times within a word or expression.

To specify a denied sender, you can enter something like “tom*@*.*” as a disallowed sender instead of individual e-mail addresses. That means that all mail sent by any Tom with any extension (such as family name) and from any domain is denied. This includes your own employee Tom Jones, to whose mails the same restrictions will be applied. To specify a particular domain, you can enter “*@domain.com”. All senders or recipients from this domain are then denied. Be careful when you create an address filtering job for multiple servers that denies an entire domain. It is not always obvious which addresses are private and which business in nature. Keep in mind that smaller companies may have e-mail addresses for example under ISP domains, such as @demon.co.uk or @aol.com.

Address filtering is a simple means for filtering out e-mails sent from known spam addresses. The usual suspects can be intercepted at the server and deleted at once.

Note: *As the processing condition is the same as the job restriction condition for address filtering, a* ***subject extension*** *– if defined – is added to passed e-mails even if the message does not meet the processing condition.*



The following actions can be performed:

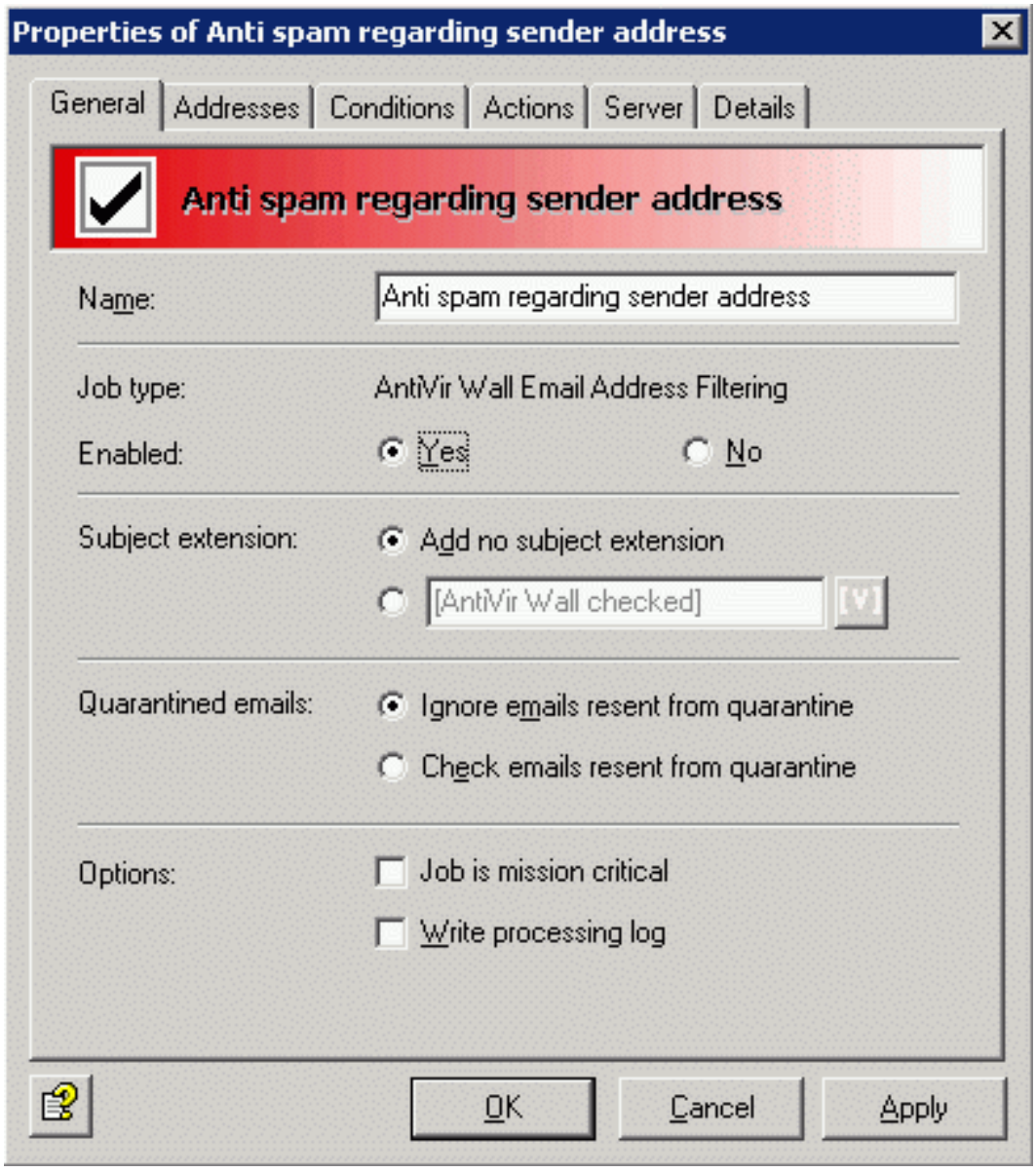
- Copy the entire e-mail to Quarantine
- Add label
- Delete the affected message without delivering it
- Notify the Administrator
- Notify the sender
- Notify the recipient
- Notify other user-defined recipients
- Start external program
- Add Avira tag and value
- Add header field and value
- Redirect mail

5.2.1 Blocking Senders and/or Recipients - Example

Under **Policy Configuration - Job Templates**, you will find a configured address filtering job. Double-click the job **Anti spam regarding sender address**, to open it.

General Settings

Under the **General** tab, enter a name for the job. An active (enabled) job has a checkmark in the icon symbol. Set the job to **Enabled: Yes**. Once you have saved your settings with **Apply** and closed the job, the job is enabled.



By default, the **Subject extension** is pre-set to **AntiVir Wall checked**. If enabled, this text is added to the subject of each mail checked by the job.

By default, the **threshold** as of which a mail is considered spam is set at 50. To avoid negative spam detection rates, it is recommended not to change this value.

This job does not process mails that are being resent from **Quarantine (AntiVir Monitor - <select quarantined email> - All Tasks - Resend quarantine item)**, even if the

Resubmit the email to all AntiVir jobs has been enabled. The **Ignore emails resent from quarantine** option means that this job is systematically skipped when a mail is resent from Quarantine.

Save the configuration of the AntiVir Exchange Management Console each time you have modified the settings. Click on the **Save** button . The configuration is saved in the ConfigData.xml file located in the Avira\AntiVir Exchange\Config\ folder. Pending changes are indicated by an asterisk (*) next to the top node.

For further information on sending quarantined mail, refer to Sending From Quarantine . For details on the **Mission Critical** option, refer to This job is mission-critical in the "AntiVir" Chapter.

Setting up Address Conditions

Under the **Addresses** tab, specify the senders or recipients to which this job is to apply. You can select addresses from existing lists or from your own ones.

For details on how to make the best use of address lists and details, refer to the description under Address Lists .

Setting up Content Conditions

Under the **Conditions** tab you can set the requirements as to which mails or documents a job is to be run for.

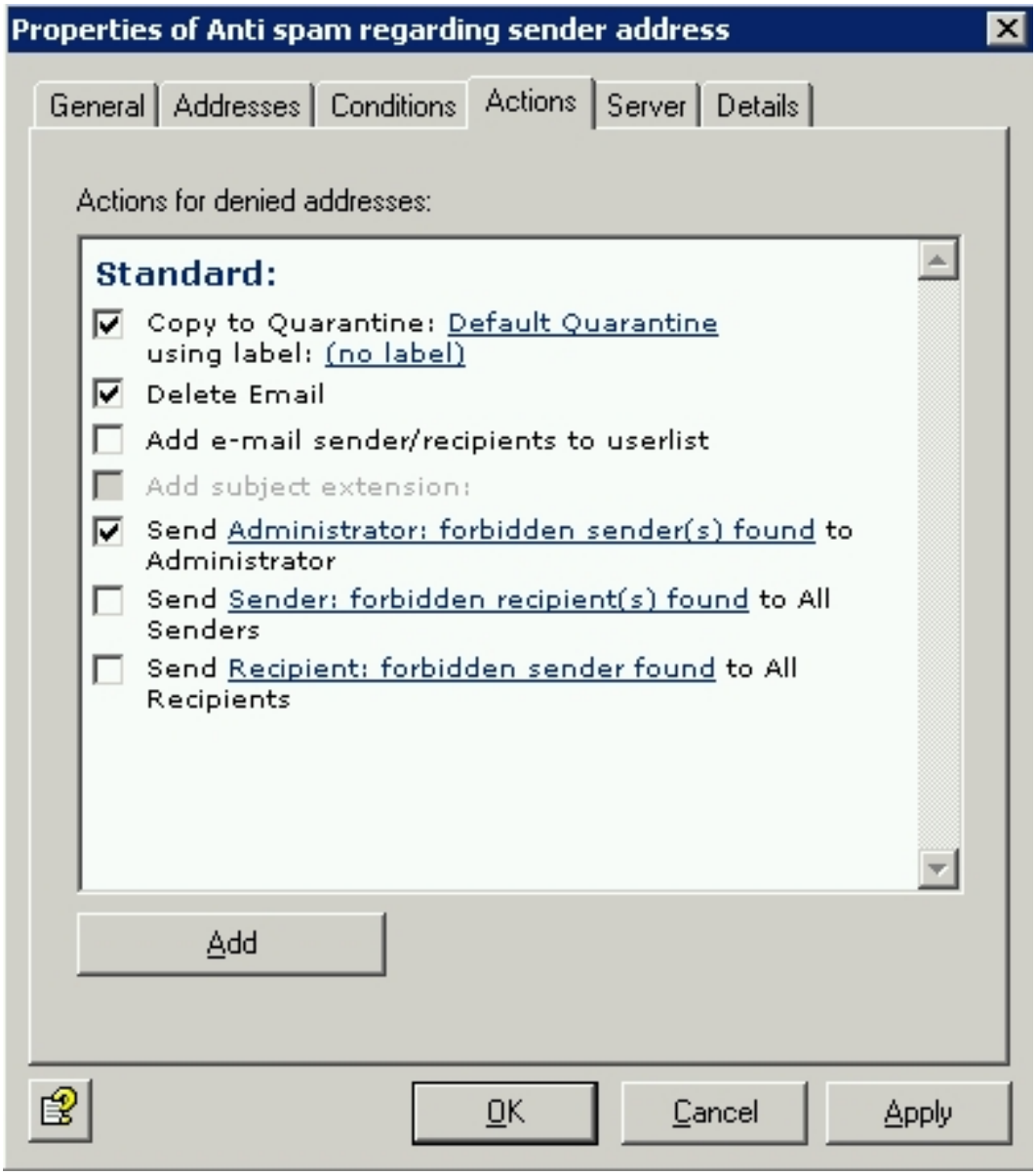
For the use and settings of conditions refer to Conditions .

Note: *The content conditions and the address conditions set in the* ***Addresses*** *tab must simultaneously come true, for a job to be run (logical AND).*

Defining Actions

Under the **Actions** tab, specify the actions to be taken when the job finds an e-mail with denied senders.

In this example, a copy of the message is placed in Quarantine and the message is deleted **without** being delivered to its recipient. A notification warning of the denied address is sent to the Administrator. You can select this notification from the pull-down menu of available notification templates, which you can format using the HTML toolbar or by entering appropriate HTML code yourself .



To define further actions, click the **Add** button.

For a description of the procedure, refer to the description in the AntiVir chapter under Enabling Virus Scanning – Example, "Defining Actions" .

Selecting Servers / Job Details

To select servers and specify job details proceed as described under Selecting Servers and Entering Job Details .

5.3 Content Filtering With Dictionaries

AntiVir Wall uses predefined dictionaries to look for undesirable text content.

It can check the following message elements:

- Subject
- E-mail text
- Attachments

Content filtering can be limited to specific senders or recipients. You can specify, for example, that only external mail is scanned for pornography, racism, etc., while own-domain mail to external recipients can be checked for internal or confidential information. Messages are scanned and compared against the specified dictionaries. When a dictionary is enabled for a particular job, the words or sentences you have entered in that list are considered restricted as of a specific threshold value. The job also defines the character conversion. When the specified threshold is reached, the job starts the actions that you have previously defined under the **Actions** tab.

The working principle of a content filtering job:

The job checks an e-mail and finds restricted content. It triggers an alarm and initiates a series of actions that you have specified for the job under Actions. Let's assume that you have specified the following

1. The message is to be moved into the Quarantine folder you have created and will not be delivered to the recipient.
2. Notifications with the relevant information from the Wall job are sent to the Administrator, the sender and the recipient.

The actions available are the same as for address filtering.

5.3.1 Setting up Dictionaries

1. Click **Dictionaries**.
2. To open a dictionary, double-click it in the right pane.
3. Under the **General** tab, enter a name for the dictionary.
4. Give the dictionary a **weighting** from 1 to 200.

   The dictionary weighting applies to each word or phrase and determines the relationship to other dictionaries and to what extent the dictionary is taken into account.

   To select servers and specify job details proceed as described under Selecting Servers and Entering Job Details .

   For further information on weighting, refer to Checking and Denying Text Contents – Example .

5. Click the input field for the words and add words and phrases that you want to forbid.

   Each word and/or phrase must stand on its own line, separated by a line break (Enter key).

   The following wildcards can be used in dictionaries:

   - Asterisk (*)

     The asterisk represents none or more characters within a word or phrase. Examples:

     `*check*` will find "check" "checkpoint", "intercheck" and "intercheckpoint".

     `check*` will find "check" and "checkpoint", but not "intercheck" nor "intercheckpoint".

The asterisk must be placed at the beginning or end of a word or phrase.

- Plus symbol (+)

  The plus symbol has the same function as the asterisk, but indicates that the search term **is part of** a word or phrase. Examples:

  `+check+` will find “checkpoint”, “intercheck” and “intercheckpoint”, but not “check” on its own.

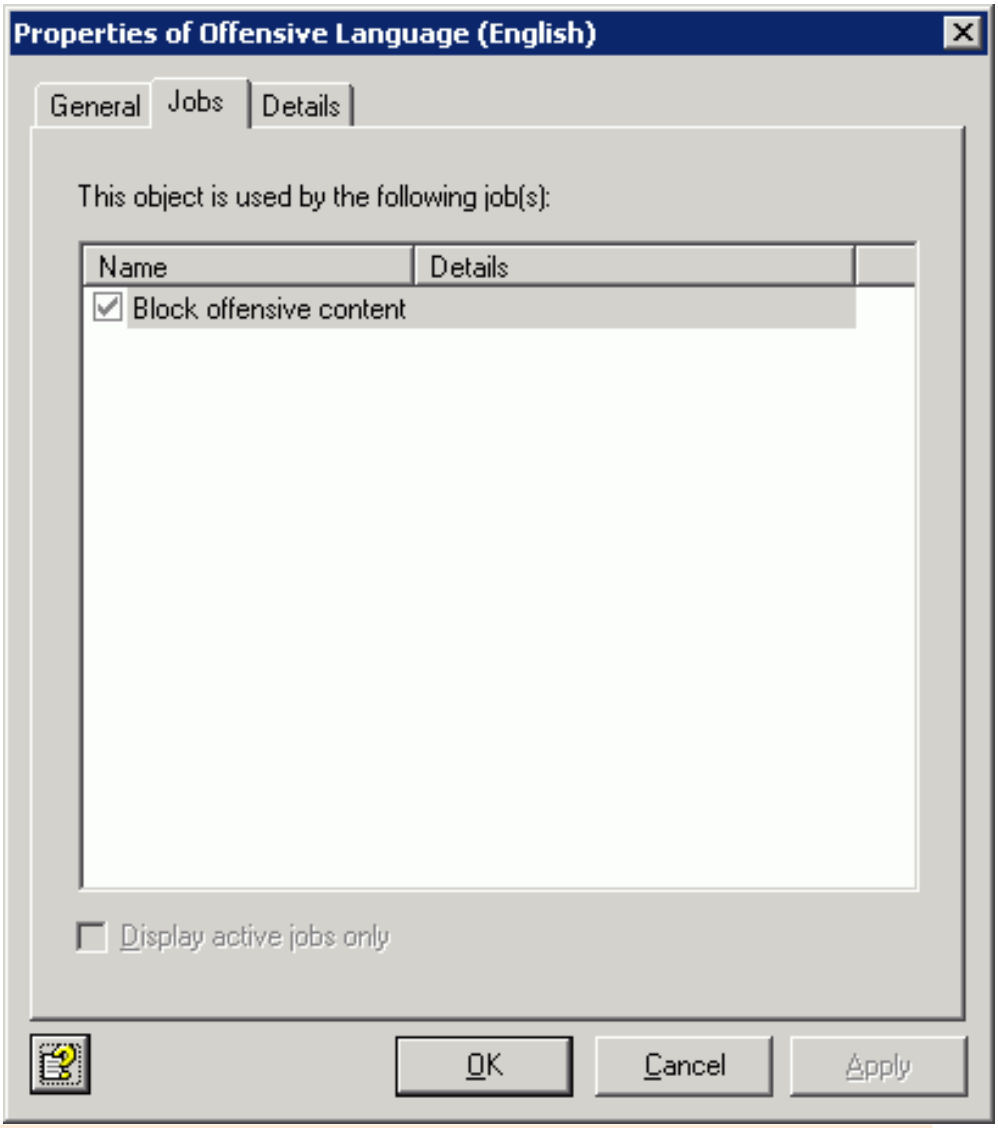
  `check+` finds only “checkpoint”.

  The plus symbol must also be placed at the start or end of a word or phrase.

Tip: *If you enter a word or phrase without wildcard, only that exact word/phrase will be found. For example, if you enter* `check`*, only the whole word “*`check`*” will be found.*

6. To sort the dictionary in ascending order, click , and to sort it in descending order, click .
7. To create a new dictionary, right-click **Dictionaries** and select **New - Dictionary**.

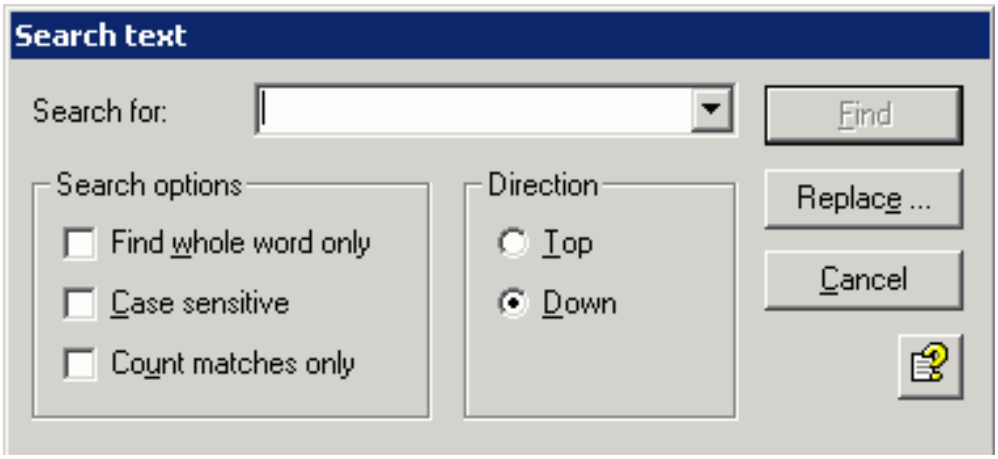
   The **Jobs** tab lists the jobs that use an object.



Note: *To use dictionaries in a job, select a Content Filtering job under Policy Configuration, enable the required dictionary and specify an overall threshold value (from 1 to 10.000). As soon as this threshold value is reached when all weighting factors (identified words/phrases) of the active dictionaries are added, the specified actions are performed. For further information, refer to Checking and Denying Text Contents - Example*

Searching for Text in Dictionaries

1. To search for and replace text in dictionaries, double-click the dictionary to open it and click :



If you do not specify any additional options, the function looks for the entered character string everywhere, i.e. also within words and phrases.

- **Find whole word only**:

  You can separate words with any non-alphanumeric character including paragraph marks and manual line breaks.

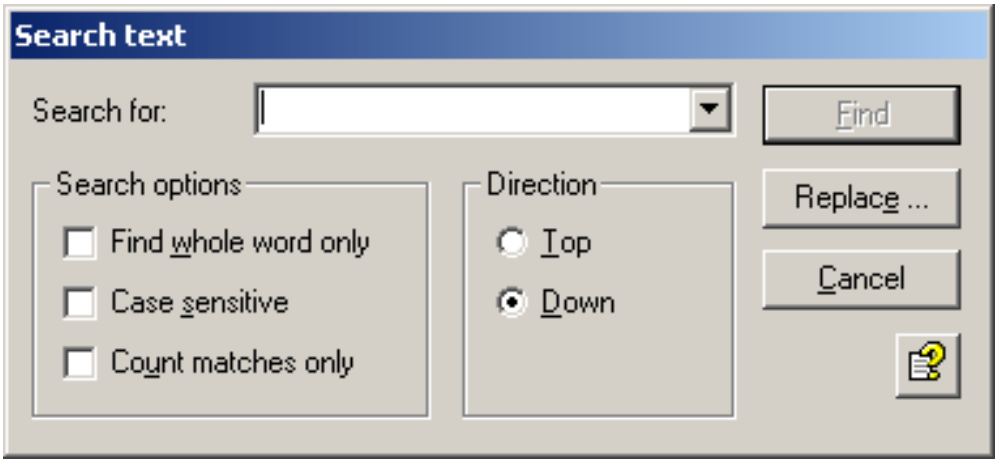
- **Case sensitive**:

  Makes the search case-sensitive.

- **Count matches only**:

  Only the number of matches is displayed, not the matches themselves:

2. To replace a string with another click **Replace**:



You can also use the text search and replace function for your own addresses. Also refer to Address Lists .

5.3.2 Checking and Denying Text Contents - Example

The **Policy Configuration - Job Templates** contains various jobs for content filtering with dictionaries.

- **Block offensive content**

  Search for obscene and pornographic language

- **Block script commands**

  Search for script commands that could cause damage

- **Block emails containing personal records**

  Search for terms common to resumés/CVs

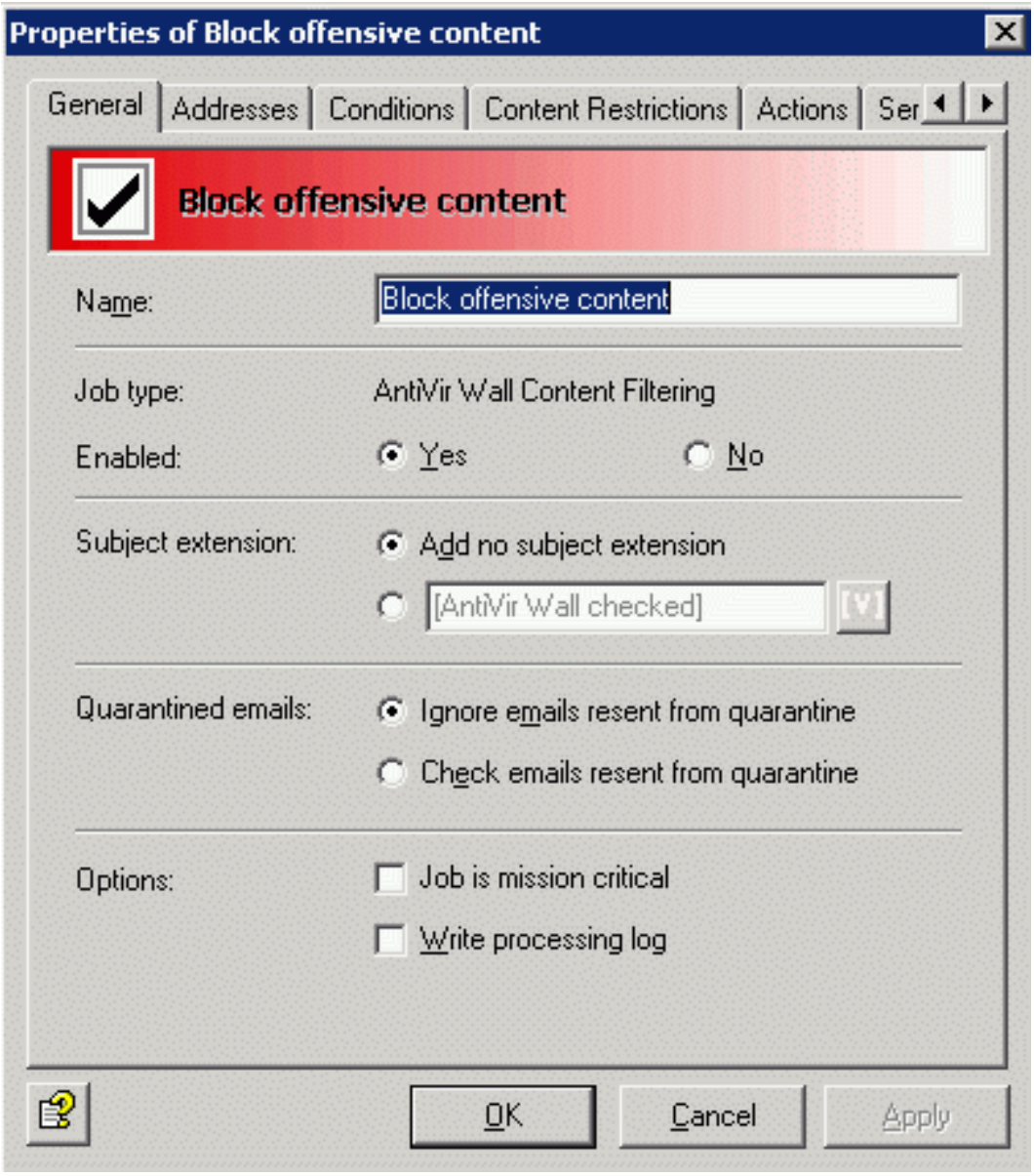
- **Block emails from the "Nigeria Connection"**

  Search for terms specific to “Nigeria” e-mails

We will use the **Block offensive content** job as an example. Drag this job to the **Mail Transport Jobs** folder and open it with a double-click.

General Settings

Under the **General** tab, enter your own name for the job. An active (enabled) job has a checkmark in the job symbol. Set the job to **Enabled: Yes**. Once you have saved your settings with **Apply** and closed the job, the job is enabled.



By default, the **Subject extension** is pre-set to **AntiVir Wall checked**. If enabled, this text is added to the subject of each mail checked by the job.

This job does not process mails that are being resent from **Quarantine (AntiVir Monitor - <select quarantined email> - All Tasks - Resend quarantine item)**, even if the **Resubmit the email to all AntiVir jobs** has been enabled. The **Ignore emails resent from quarantine** option means that this job is systematically skipped when a mail is resent from Quarantine.

For further information on sending quarantined mail, refer to Sending From Quarantine . For details on the **Mission Critical** option, refer to This job is mission-critical in the "AntiVir" Chapter.

Setting up Address Conditions

Under the **Addresses** tab, specify the senders or recipients to which this job is to apply. You can select addresses from existing lists or from your own ones.

For details on how to make the best use of address lists and details, refer to the

description under Address Lists .

Setting up Content Conditions

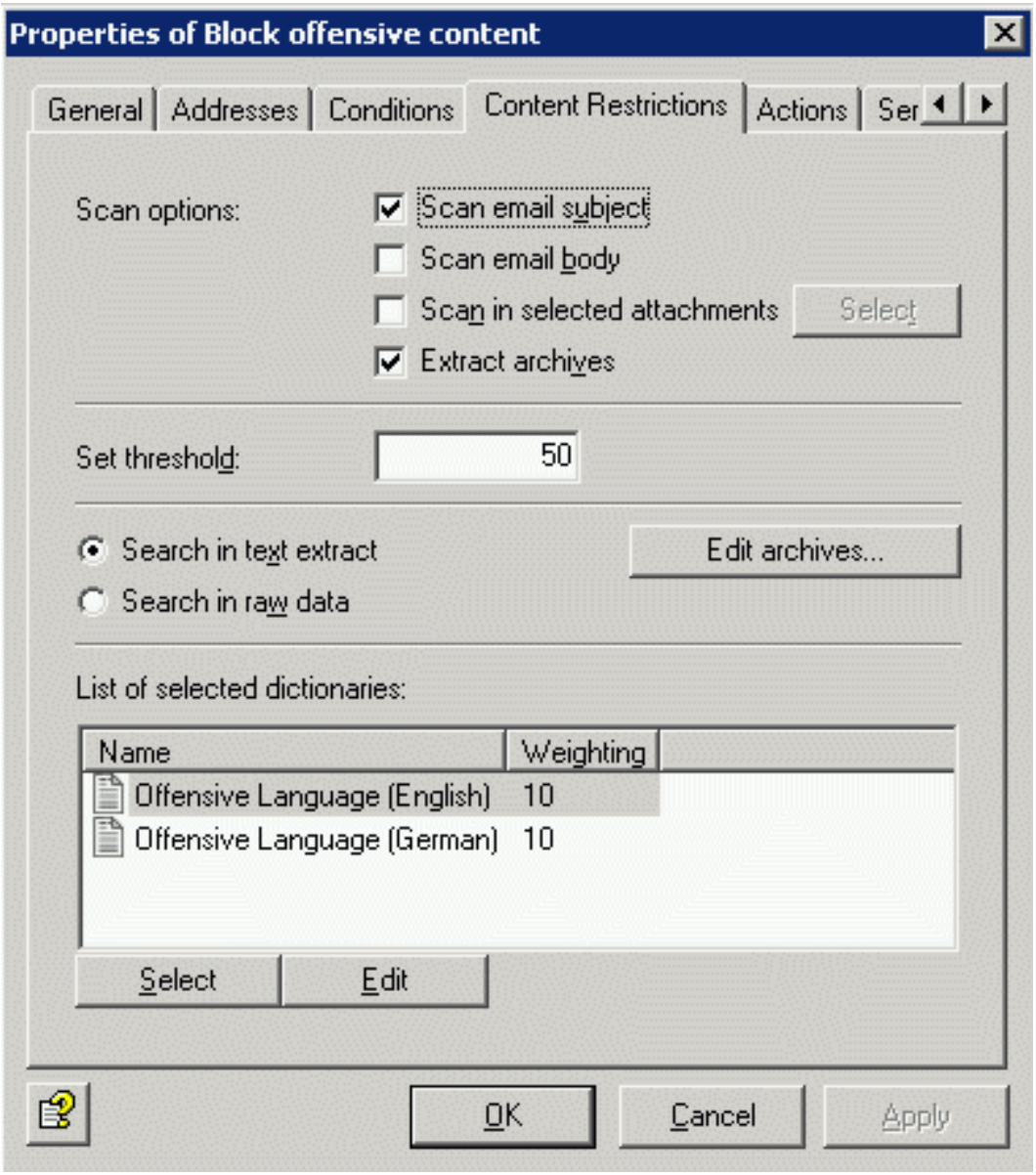
Under the **Conditions** tab you can set the requirements as to which mails or documents a job is to be run for.

For the use and settings of conditions refer to Conditions .

Note: *The content conditions and the address conditions set in the* ***Addresses*** *tab must simultaneously come true, for a job to be run (logical AND).*

Selecting Dictionaries

Under the **Content Restrictions** tab, specify the dictionaries to be used by this job.



This job checks the subject line. The overall threshold value is set to 50. This means that when five words/phrases from the **Offensive Language (English)** or **Offensive Language (German)** dictionary have been found, the specified actions are performed.

Calculation: Every word or phrase in the **Offensive Language** list has a value of 10. In this example, the threshold of 50 is reached when at least five words from these lists are found in the message.

Explanation: Every word or phrase in the **Offensive Language** list has a weighting of 10. Each word or phrase from this list found is counted and multiplied with the weighting and finally compared to the threshold value.

In this case: Let's assume that 5 words from the dictionary were found in the message. The sum of these words is multiplied with the weighting (10): 5 × 10 = 50. This value is compared to the threshold value. Since this is also 50, the action is executed.If only 4 words are found in the message, the total value is 40 (4 x 10), which is less than the threshold value, and no action is triggered.

You are using **two different dictionaries** for checking the subject and the message body for denied content.

The **overall threshold** value for the job is set to 20 and the first dictionary (A) specified in the job has a weighting of 20. The second dictionary (B) specified in this job has a weighting of 1. This means that the specified actions are performed when one word or phrase from the dictionary A or 20 terms from the dictionary B are found.

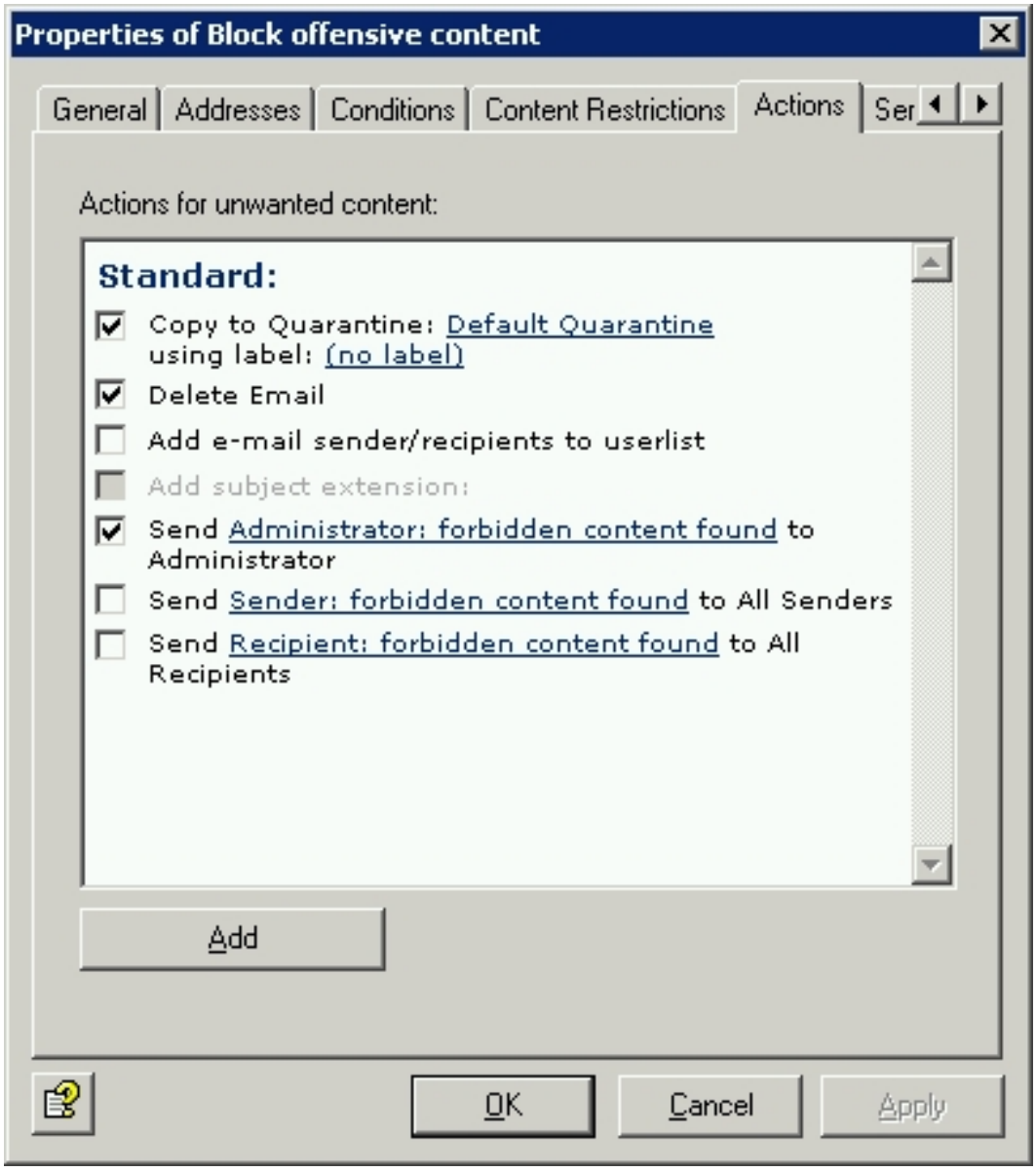
The threshold is calculated as follows: Every word or phrase in the first word list A has a weighting of 20. If an e-mail contains only a single phrase from this list, the threshold value is reached and the action is performed.

Every word or phrase in the second word list B has a weighting of 1. Each word or phrase from this list found is counted and the sum of them multiplied with the weighting. The found value is then compared to the threshold value. If, therefore, 21 words from the dictionary B are found in the message, these are multiplied by the value (1): 21 × 1 = 21. the sum is compared to the threshold value. Since this is 20, the action is executed.

Tip: *To handle content in different languages, create the appropriate Dictionaries and define one job for each language. For languages such as French and Spanish, define your own character conversion table. For further information on creating your own schemes, please contact our Support.*

Defining Actions

Under the **Actions** tab, specify the actions to be taken **when the job finds an e-mail with denied content**.



In this example, a copy of the message is placed in Quarantine and the message is deleted **without** being delivered to its recipient. A notification that the corporate policy was breached is sent to the Administrator. You can select this notification from the pull-down menu of available notification templates, which you can format using the HTML toolbar or by entering appropriate HTML code yourself.

Save the configuration of the AntiVir Exchange Management Console each time you have modified the settings. Click on the **Save** button . The configuration is saved in the `ConfigData.xml` file located in the `Avira\AntiVir Exchange\Config\` folder. Pending changes are indicated by an asterisk (*) next to the top node.

5.4 Anti-Spam with the AntiVir Wall Spam Filtering Job

Spam Filtering scans e-mails for characteristics typical for spam. Unlike virus-infected mail, spam is not always clearly identifiable as such. Unsolicited mail can hold a wide variety of content and its originators use various methods to disguise it as “normal” mail to avoid its detection by spam filters.

Any spam filtering job therefore has to take into account that e-mails may not be definitely identifiable as spam. The spam filtering job works with a range of different criteria for identifying spam. These criteria are split into definite and combined criteria.

Using the definite criteria, the job scans mail for unique spam characteristics and classifies them into spam and non-spam. It then uses the combined criteria to investigate the “gray zone” and determine a likelihood of the checked message being spam – its spam probability. The spam probability for the definite criteria is always 0 % or 100 %, while the probability for the combined criteria can range from 1 to 99.You will find a configured **Advanced spam filtering** job under **Policy Configuration - Job Templates**. The job carries out a range of analyses and checks the following elements of each e-mail:

- E-mail headers
- Subject
- E-mail text

Like in normal content filtering, e-mails are checked for characteristic spam texts using dictionaries.

In the “gray zone”, some of the characteristics typical for spam occur more frequently while others suggest that an e-mail may not be spam. On their own, combined criteria only pick up particular characteristics of an e-mail that suggest that it may be spam. The greater the number of characteristics that match the combined criteria, the greater the likelihood that the message is spam. The identified characteristics are combined (hence “combined criteria”) to obtain a value indicating the probability that the message is spam.

Tip: *The defined job is configured so that a high* ***spam probability*** *– for example over 91 % – can be achieved only when definite spam characteristics have been identified by several combined criteria.*

The job distinguishes between up to four spam probability ranges. The boundaries between these ranges (i.e. the probability threshold values) are user-definable with sliders. For each range, you can specify actions to be taken for e-mails that fall into that range. For example, you can specify that:

- definite "non-spam" with a **Spam probability** of 0 % is delivered as normal;
- e-mails with a spam probability below 10 % are also delivered as normal. You may want to place e-mails for classification in the **Spam Low** Quarantine
- for mail with a spam probability between 10 and 50 %, the **SCL field** is processed in Exchange 2003, so that the e-mail is automatically moved to the recipient’s junk mail folder or the e-mails are placed into the **Spam Middle** Quarantine;

  - the recipients receive a summary report on the quarantined e-mails and can request their delivery if required;

- e-mails with a spam probability over 50 % are deleted immediately. Here, too, you can place e-mails in the **Spam High** Quarantine.

The following actions can be performed:

- Copy the entire e-mail to Quarantine
- Add label
- Delete the affected message without delivering it
- Add the email sender or recipients to userlist
- Notify the Administrator
- Notify the sender
- Notify the recipient
- Notify other user-defined recipients
- Start external program
- Add Avira tag and value
- Add header field and value

- Redirect mail

The individual thresholds are:

1. **Spam Probability: None**. Default: 0.
2. **Spam Probability: Low**. Default: 0 - 9.
3. **Spam Probability: Medium**. Default: 10 - 49.
4. **Spam Probability: High**. Default: 50 -100.

The **Low**, **Medium** and **High** ranges can be adjusted with sliders and linked to corresponding actions, which are then performed on all e-mails in that range. For spam probability **None**, you can specify a **subject extension**.

In addition to effective spam filtering, an anti-spam solution must prevent the incorrect classification of mail as spam (false positives) and use the available processing resources efficiently in productive use. Mail is therefore checked using the **definite criteria** before the combined criteria are applied, so that e-mails that can be definitively classified as spam or non-spam are not subjected to further analysis. The exclusion criteria prevent checking e-mails that can be definitely identified as non-spam, for example through their sender.

Note: *When a definite criterion applies, the spam probability is always 0 % or 100 % and therefore falls into the probability range* ***None*** *or* ***High****, for which the corresponding actions are performed.*
Note: *Of course, these criteria do not affect the execution of the remaining enabled jobs, such as attachment checking by AntiVir. Thus, if you have enabled the definite "No spam" criterion* ***E-mails with attachments*** *and set the threshold value (****Minimum number****) to 2, this means only that the Spam Filtering job immediately places these e-mails into the* ***None*** *spam probability range and not that a AntiVir job will let those two attachments pass into your network unchecked.*
Note: *Normally you do not have to adapt the combined criteria. If your spam detection rate is unsatisfactory, try optimizing the definite spam criteria (see below for exclusion criteria).*

5.4.1 Definite No-Spam Criteria

You can define the following exclusion criteria in the job:

Criterion	Description
E-mails from these trusted senders (Whitelist)	Whitelist: addresses of all known senders that are always allowed and that are known not to send spam. This normally includes all regular communication partners as well as the domains of your customers and suppliers. Keeping this list up-to-date and comprehensive ensures that your system resources will not be burdened with unnecessary checking.
E-mails from Active Directory users	All of the users and contacts included in the Active Directory are regarded as trustworthy.
E-mails from User Whitelist entries	The senders (address entries) included in the user whitelist are delivered without prior checking for spam.
Emails containing attachments	E-mails with file attachments. Most unsolicited mail does not contain attachments. You can optionally

Criterion	Description
	enter a threshold value here. Example: Minimum number = 2 means that all messages with two or more file attachments are delivered without spam checking.
Emails with minimum size of	Spam e-mails are generally small, and large e-mails are therefore unlikely to be spam. Here, you can enter a size above which message are no longer checked for spam.
Emails in TNEF format	TNEF E-Mails. This Exchange-specific format is not being used by spammers yet.
Emails encrypted and/ or signed	Encrypted and/or signed e-mails. Spammers do not send encrypted or signed e-mails.
Microsoft Exchange "No spam" SCL value Also refer to Write spam result in Exchange SCL field .	Spam confidence level (SCL), spam filter (intelligent message filter – IMF) from Exchange 2003. SCL accepts integers from -1 to 9. Exchange assigns -1 for e-mails from senders from the same Exchange organization. The Wall Spam Filtering job treats this value as definite “no spam” criterion.

5.4.2 Definite Spam Criteria

Criterion	Description
E-mails from the following senders (Blacklist)	Blacklist: All sender addresses known to be originators of spam. The default configuration contains a list of known addresses to which you can add further addresses.
Emails with this character set	This function checks the charset field in the message header for the character sets in the specified list. Messages with a matching character set are immediately classified as spam.
Exchange SenderID request returns "FAIL" For details on SenderID refer to http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx	If enabled, the mail's sender ID is also checked. This allows to prevent "spoofing", i.e. the falsification of sender mail address domains. The analysis is based on entries in a DNS, which is used to determine from which iP addresses e-mails from specific domains are allowed to be sent or not. The Sender ID result is provided with the mail. Wall checks the mail's Sender ID and classifies the result "FAIL" as spam. To be able to use the SenderID function, a number of other functions need to be enabled at the server, such as the associated SenderID filter. The filter is enabled under **Server - Protocols - SMTP - Properties** in the **Identification** field. In addition, both server and client (Outlook) must be configured.

Tip: *If you want e-mails deleted immediately only if they are definitely spam, set the* ***spam probability*** *for* ***High*** *to 100 and define an appropriate action. This ensures that only e-mails definitely identified as spam (i.e. using the blacklist or character set) fall into this range. If you set this range, for instance, to 91 to 100, e-mails with a high spam probability based on other criteria will also be placed into this category.*

5.4.3 Practical Tips

Depending on your working environment, the job may sometimes classify normal and wanted mail as spam. If that happens, try the following configuration settings:

1. If the affected e-mails all exceed the spam probability threshold by only a small amount, increase the threshold value to avoid false positives.

2. If e-mails from a particular sender are regularly classified incorrectly as spam, add this sender to the Active Directory or the whitelist (under **Definite Criteria - No Spam**), so that these e-mails are no longer checked for spam.

3. Try to identify terms and expressions typically used in the affected e-mails and enter them in the Business Words dictionary. These words will then be taken into account through the “No Spam” criterion **Body business phrases** so that e-mails containing them will receive a lower spam value.

4. If the number of false positives is still unacceptably high after you have taken the above measures, try to identify which criteria have caused the incorrect classification. To do so, you can use the Cause Description in the Quarantine or the **AntiVir Wall: Spam analysis details** label variable. If the same criterion is always responsible, reduce its significance by reducing the **relevance** of this criterion by one level under **Combined Criteria**. This criterion then has a lower relevance in determining the spam probability of e-mail.

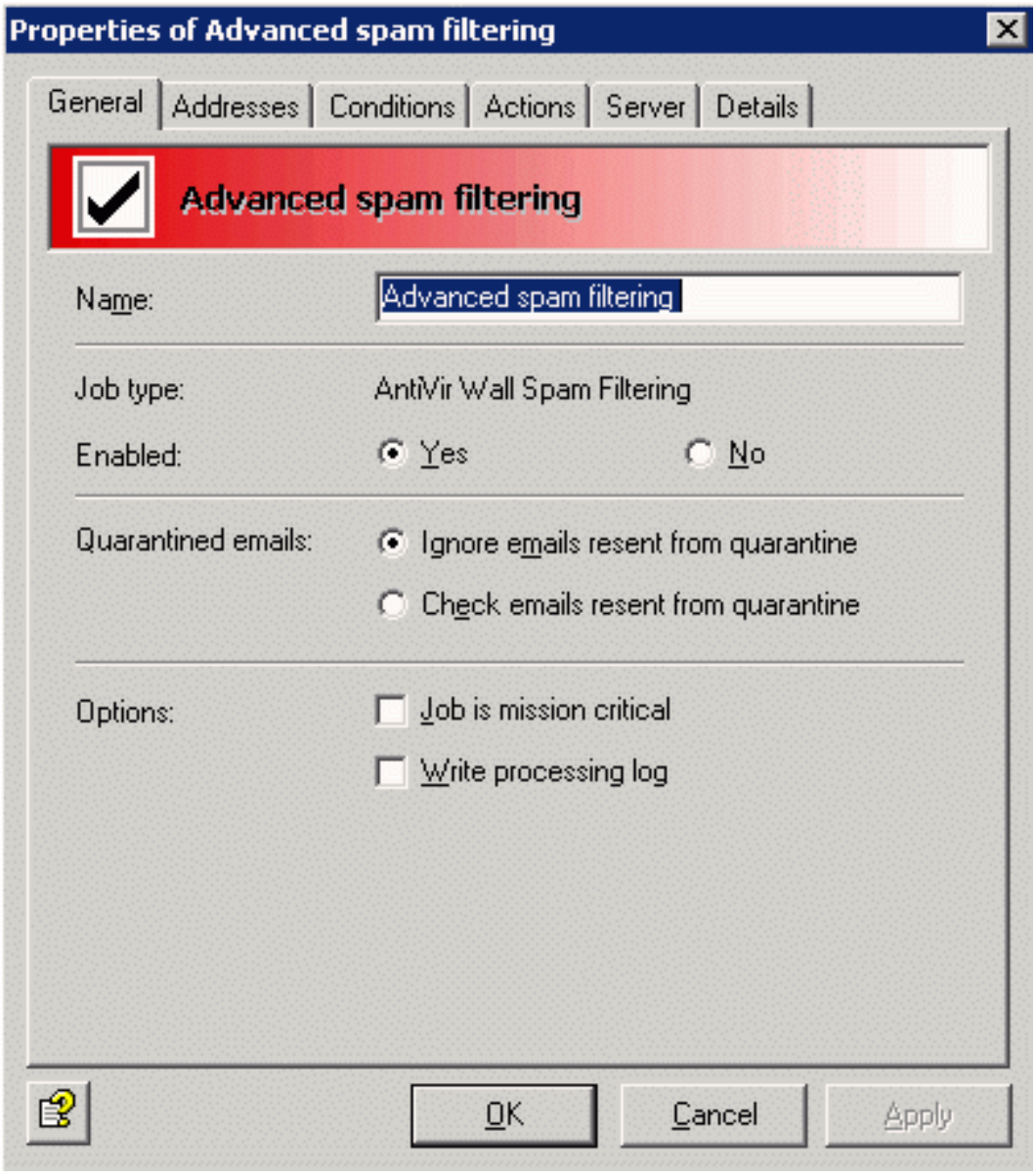
5. If you are sufficiently familiar with the characteristics of typical e-mails in your business environment (both spam and non-spam), you can also use the **Combined Criteria** under **Advanced Configuration** to optimize each criterion for your environment. This is especially useful if you had to reduce the relevance of a criterion by a large amount or disable it altogether to prevent false positives. This can, however, result in a reduced effectiveness of the spam filter. For further information, refer to Advanced Spam Filtering .

5.4.4 Spam Filtering - Example

Under **Policy Configuration - Mail Transport Jobs**, you will find a configured Spam Filtering job. Double-click the **Advanced Spam Filtering** job to open it. This job scans the e-mails for special spam features.

General Settings

Under the **General** tab, enter a name for the job. An active (enabled) job has a checkmark in the job symbol. Set the job to **Enabled: Yes**. Once you have saved your settings with **Apply** and closed the job, the job is enabled.



This job does not process mails that are being resent from **Quarantine (AntiVir Monitor - <select quarantined email> - All Tasks - Resend quarantine item)**, even if the **Resubmit the email to all AntiVir jobs** has been enabled. The **Ignore emails resent from quarantine** option means that this job is systematically skipped when a mail is resent from Quarantine.

For further information on sending quarantined mail, refer to Sending From Quarantine . For details on the **Mission Critical** option, refer to This job is mission-critical in the "AntiVir" Chapter.

***Tip:** In this job, the **Subject extension** field is located under the **Actions** tab.*

Setting up Address Conditions

Under the **Addresses** tab, specify the senders or recipients to which this job is to apply. You can select addresses from existing lists or from your own ones.

For details on how to make the best use of address lists and details, refer to the description under Address Lists .

Setting up Content Conditions

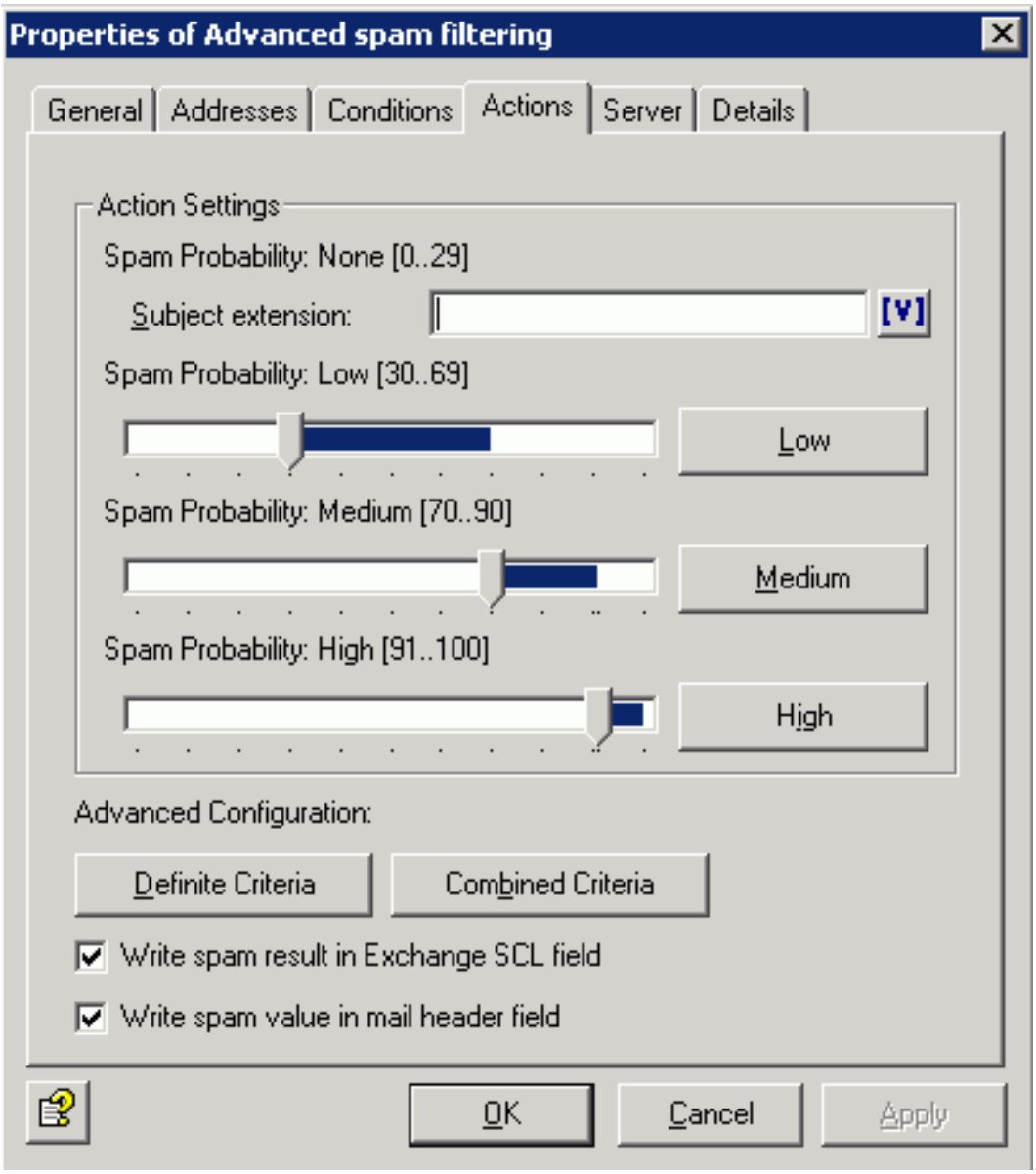
Under the **Conditions** tab you can set the requirements as to which mails or documents a job is to be run for.

For the use and settings of conditions refer to Conditions .

Note: *The content conditions and the address conditions set in the* ***Addresses*** *tab must simultaneously come true, for a job to be run (logical AND).*

Defining Actions

Under the **Actions** tab, specify the spam probabilities and the action to be taken on identified spam e-mails.



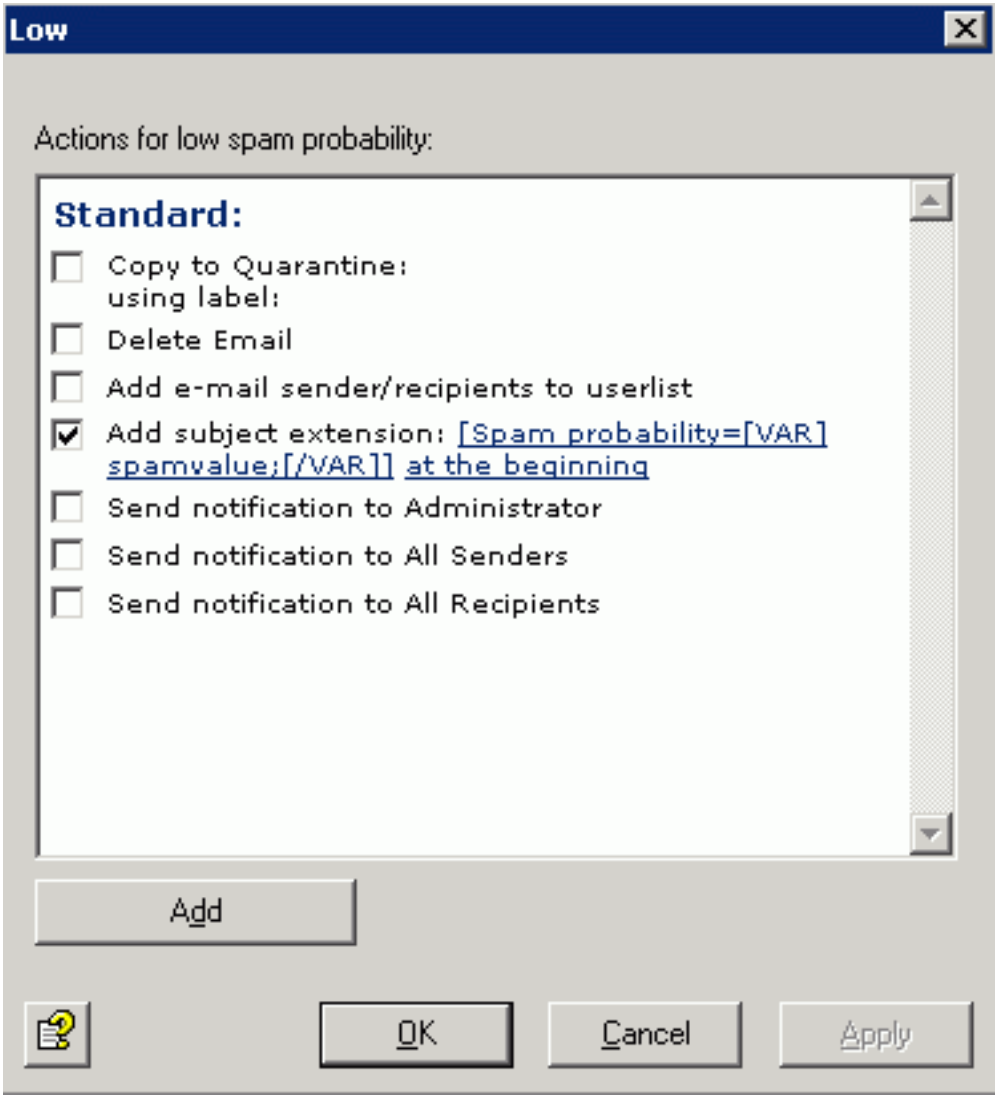
In this example, the following spam probabilities are specified:

- In the **Spam Probability: None** (value here = 0-29) range, no actions are usually

performed. The only possible action in this probability range is to add a **Subject extension**, which you can define on this tab. You could, for example, enter `Checked for spam`.

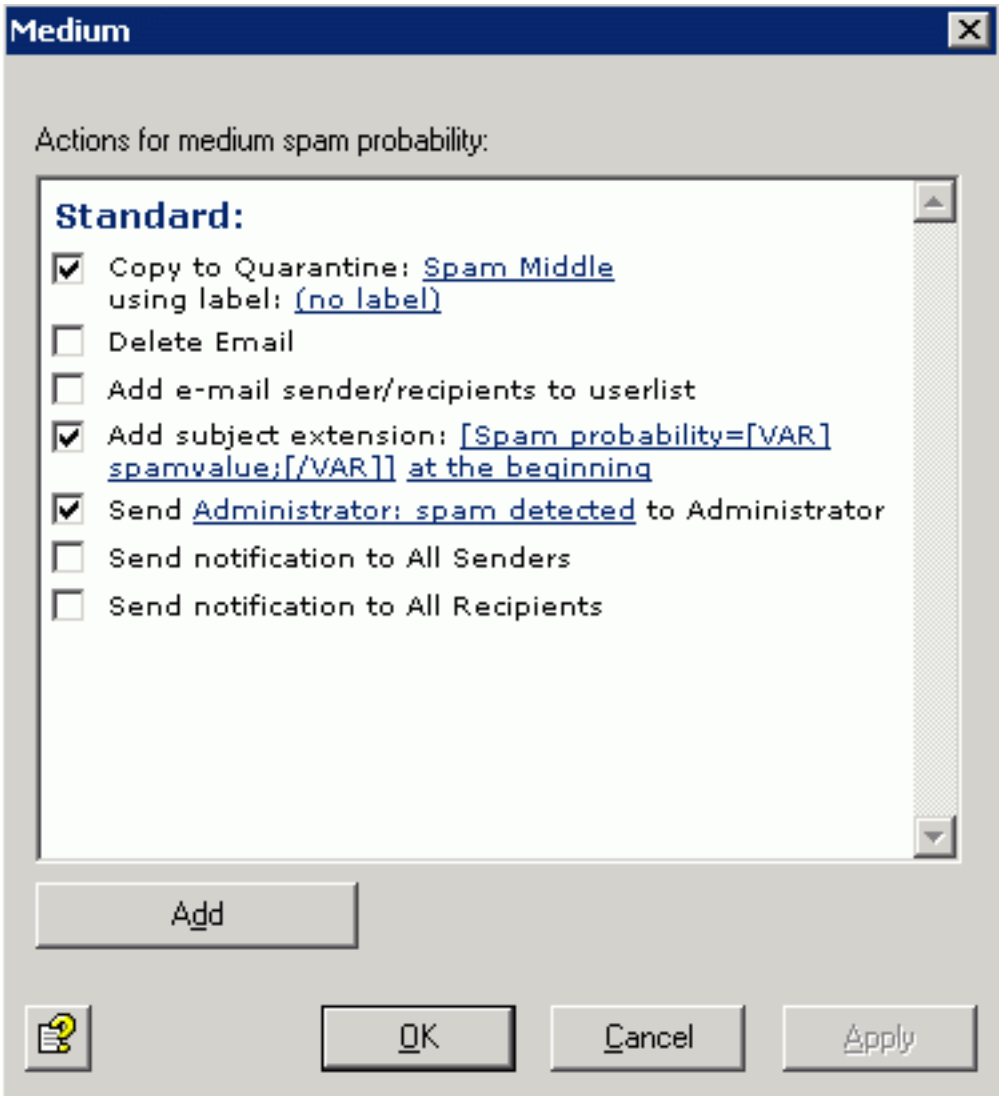
- In the **Spam Probability: Low** (here: 30 to 69) range, the actions are defined on a separate tab. Click the **Low** button.

  The following dialog appears:



The only action defined in this example is to add the probability as subject extension.

To configure the actions for the **Spam Probability: Medium** range (set here from 70 to 90), click the **Medium** button. The following dialog appears:



The actions defined here are: place a copy of the message into Quarantine, notify the Administrator, deliver the original message to its recipient, adding a **subject extension** to notify the recipient of the spam probability of this message (e.g. Spam probability = 75). The higher this value, the greater the likelihood that this is not a high-priority message. The Spam probability **Medium** is for those mails that may or may not be spam. The low values of this setting mean that a medium spam probability is assumed if a few criteria suggesting a great spam likelihood or many criteria suggesting a small likelihood of spam were found. We recommend to store these e-mails in a separate Quarantine (**Spam Middle**) and to let the recipients decide what to do with them.

Tip: *Summary reports can be used to notify users of quarantined spam mails addressed to them. You can also use the Microsoft SCL value to forward the e-mails directly to the users' junk folder through the Exchange Store (see next section). If you have a* ***Subject extension*** *defined to display the spam probability value, users can set up their own Outlook message rules to deal with the mail.*

Write spam result in Exchange SCL field

As of Service Pack 1 for Exchange 2003 and Outlook 2003, Microsoft supplies a spam filter. This Intelligent Message Filter (IMF) determines a spam probability – the so-called Spam Confidence Level (SCL) – from -1 to 9. The higher the spam probability, the larger the SCL. An SCL of 0 means that the message is probably not spam -1 is used for unfiltered mail, for example internal mail from senders in the same Exchange organization. The Exchange SCL value trigger specified actions, such as automatically

moving message to the user's Outlook junk mail folder. In the Exchange System Manager, you can centrally define what is to be done with e-mails with SCL values above a set threshold. You do not have to specify the action on the same system that assigns the SCL. As the IMF assigns the e-mails' SCL value, any defined actions can be only be performed on the target system. To that end, the e-mail gateway must also run Exchange 2003.

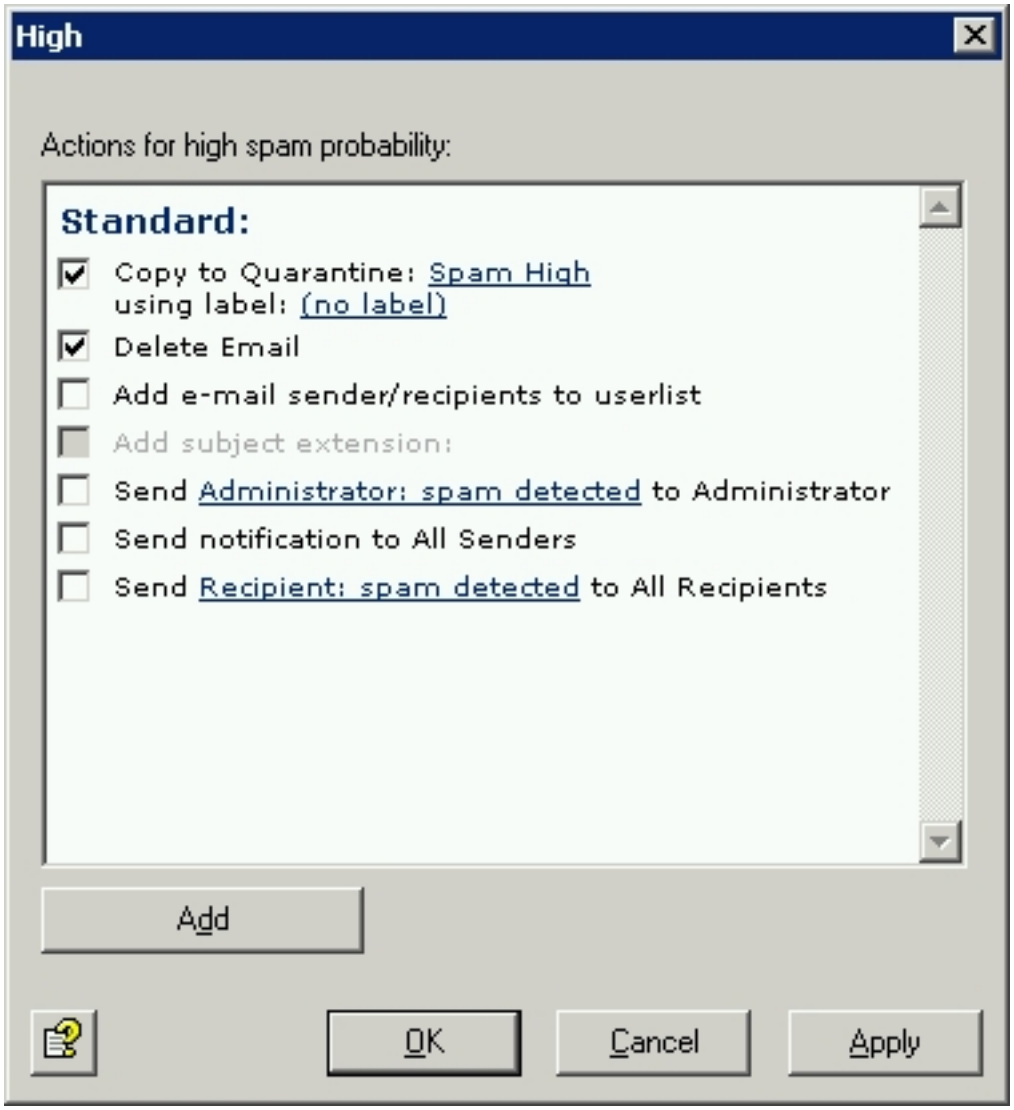
Even if you do not use the IMF, you can use this option to define the spam probability value for the spam filtering jobs as SCL result, so that they can use Exchange Store functionality for further processing. The spam probability values are internally converted to SCL values, which Outlook can use.

Tip: *If you are using the summary report function, users are notified of all relevant spam e-mails. In that case you do not have to use Exchange Store forwarding to junk mail folders. For further information on the Exchange SCL field, visit http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/imfdeploy.mspx*

Write spam value in mail header field

The spam probability value (low, medium and high) is always written in the mail header. The result is converted to a string of asterisks (one asterisk meaning a value up to 10, two asterisks a value up to 20, three asterisks up to 30, etc.) to which an Outlook rule can be applied. You can also specify the result separately for each Spam probability: In the **Actions** tab, select **Add - Add X-header** field. The result is then output as a numeric value instead of being converted to a string of asterisks.

To configure the actions for the **Spam Probability: High** range (set here from 91 to 100), click the **High** button. The following dialog appears:



The Spam probability **High** is intended for those e-mails that are probably spam and should not be delivered. In this example, the original message is deleted immediately without being forwarded to its recipient. A copy of the message is placed in the Quarantine. Because of today's large numbers of junk mail, the Administrator is not notified.

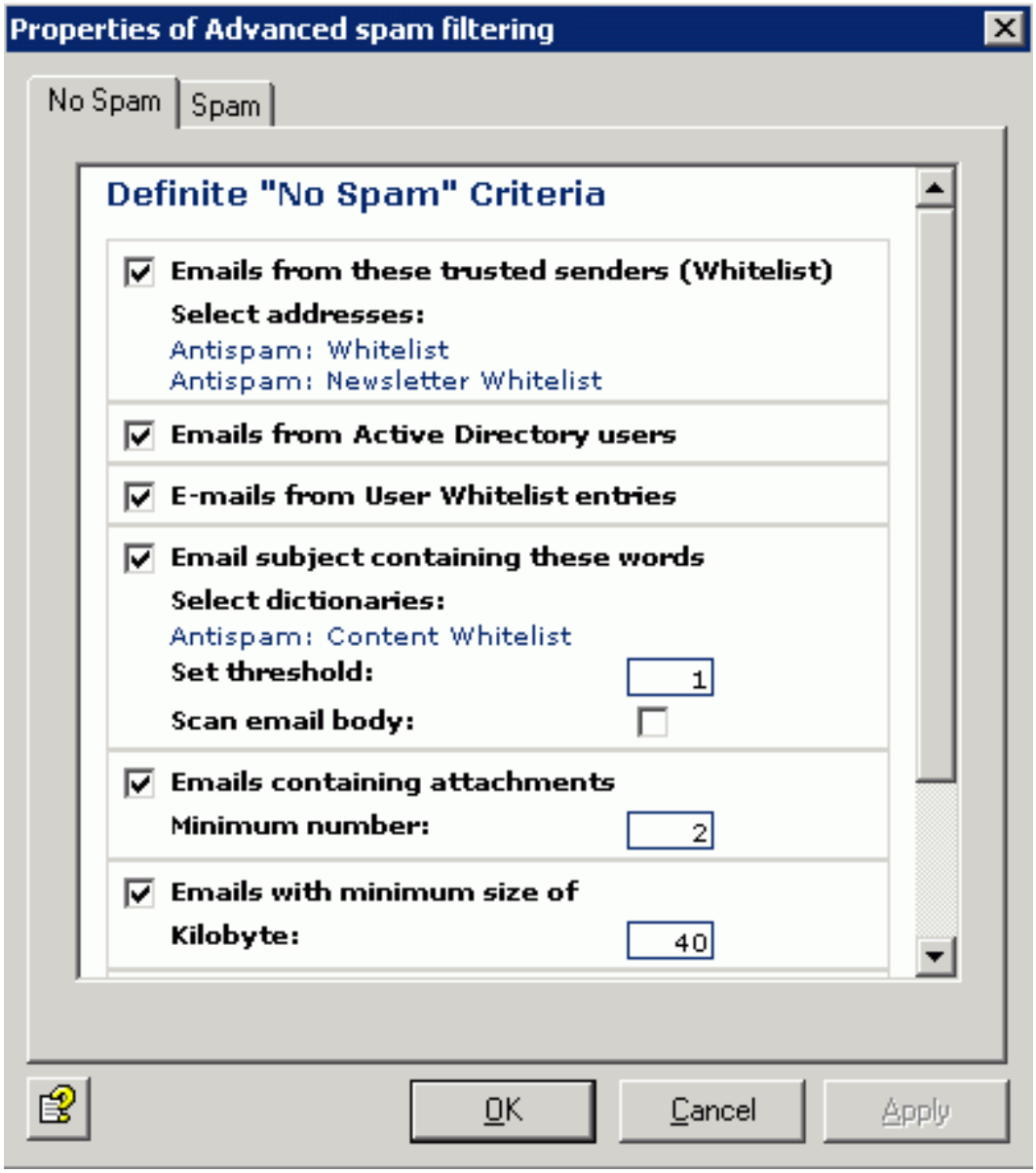
Note: *A high volume of junk mail can result in large quarantines, which can reduce system performance. When you no longer need the e-mails, you should therefore disable the Low and High Quarantine copy.*

Tip: *Depending on your mail environment, you may want to set different threshold values for the **Medium** and **High** ranges. Before you do change the thresholds, though, observe whether the job yields good filtering results with these settings.*

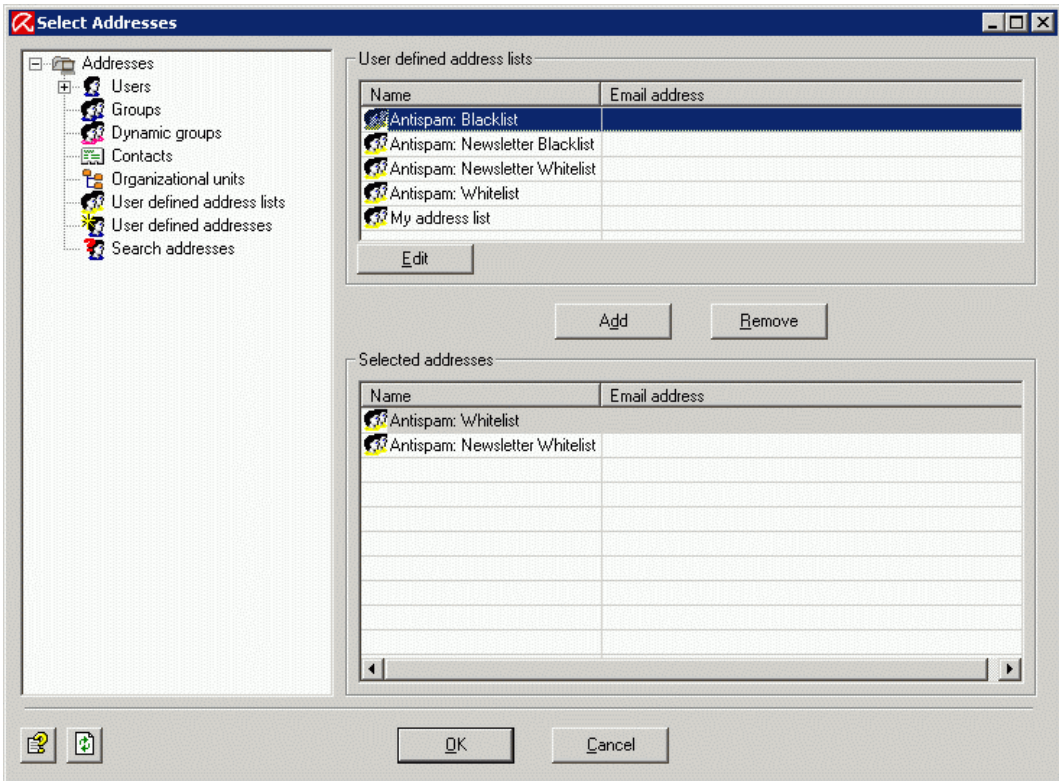
Your aims should be:

- to maximize the number of spam e-mails in the **Spam High** Quarantine,
- to maximize the number of ham e-mails in the **Spam Low** Quarantine,
- and therefore to minimize the volume of mail going into the **Spam Medium** Quarantine.

On the **Actions** tab you can adjust the spam criteria. Click **Definite Criteria**. The following dialog appears:

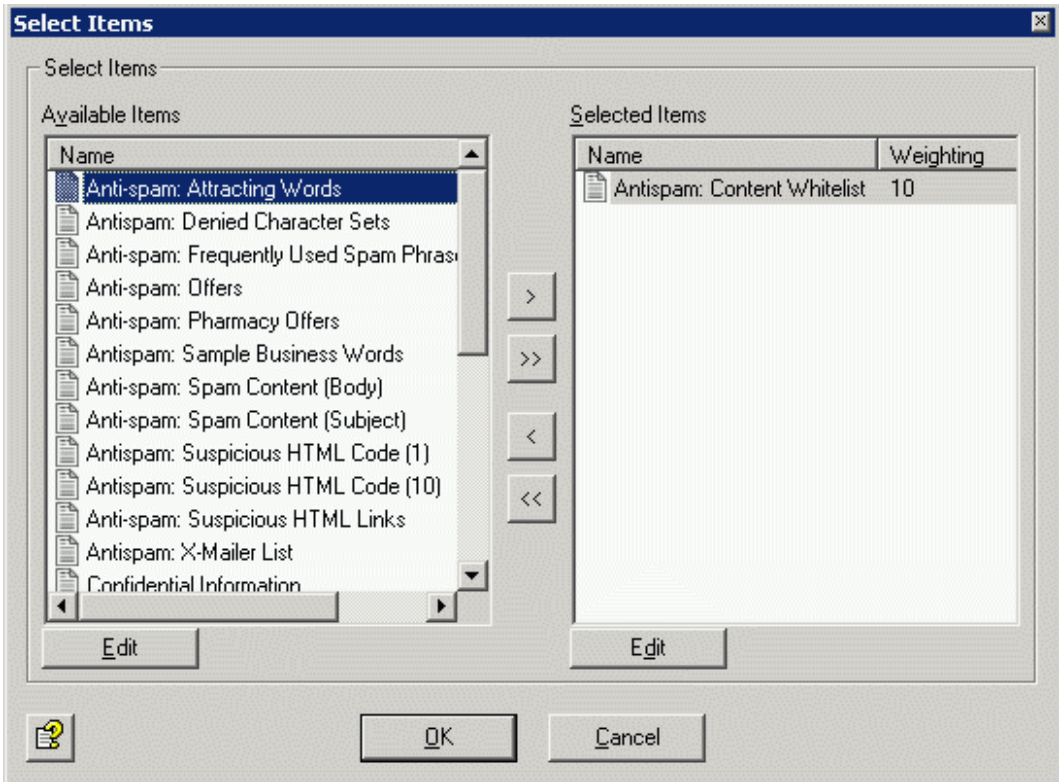


If you want to systematically allow e-mails from specific senders, click **Antispam: Whitelist** and **Antispam: Newsletter Whitelist** in the criterion **Emails from these trusted senders (Whitelist)**. The address selection dialog appears:



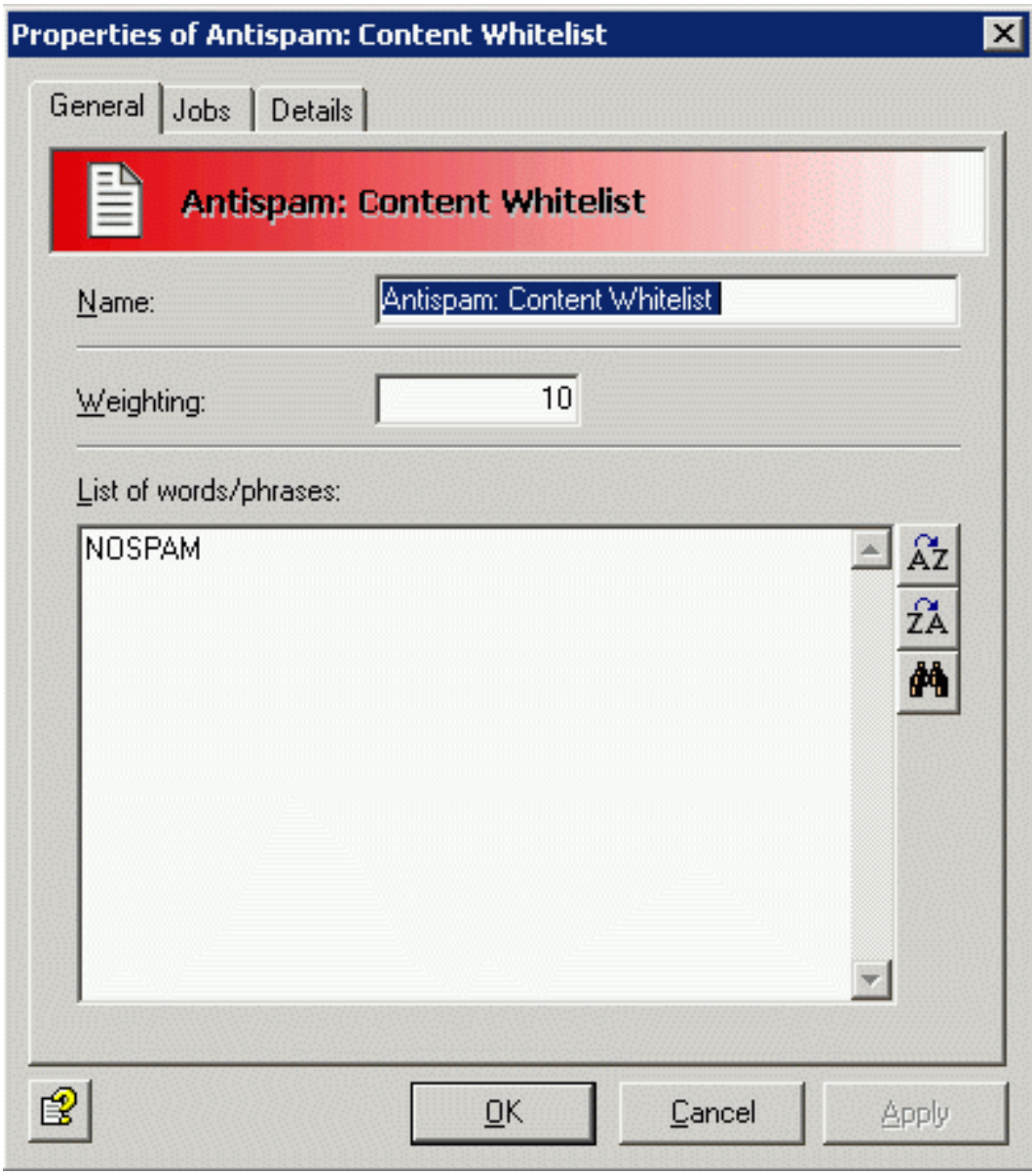
Select or enter the addresses that are to be always allowed as sender. You can use the asterisk (*) and question mark (?) as wildcard. Alternatively, you can specify entire domains in the form `*.domain.com`. After having entered all addresses, click **OK**.

In the Definite “No Spam” Criteria dialog, you can now customize the next criterion, **Email subject containing these words**. Click **Antispam: Content Whitelist**. The Dictionary Selection dialog appears:



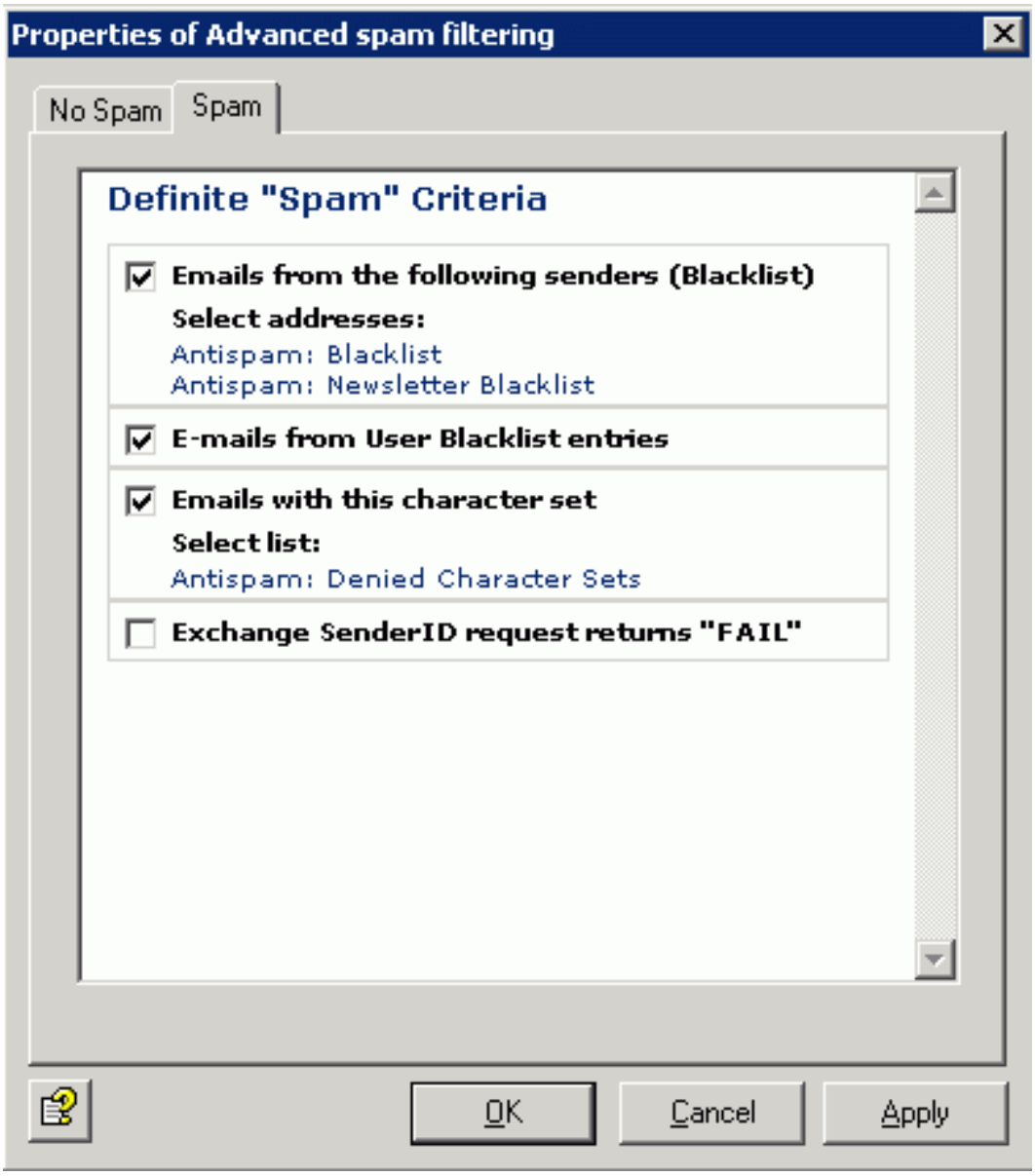
Use the < and > arrow keys to add and remove dictionaries in the list. The double arrows add or remove all existing dictionaries. In the right field, double-click **Antispam: Content Whitelist** or click the **Edit** button.

The following dialog appears:



For further information on setting up dictionaries refer to Setting up Dictionaries . For a detailed description of the remaining criteria refer to Definite No-Spam Criteria .

When you have completed the dictionary and confirmed your input twice with **OK**, click the **Spam** tab:



In the **Emails from the following senders (Blacklist)** field, click **Antispam: Blacklist** and **Antispam: Newsletter Blacklist**. An address selection dialog appears, in which you can enter e-mail addresses or domain names.

Note: *Make sure you keep both the whitelist and the blacklist up-to-date.*

In addition, by selecting a particular character set, you can declare e-mails from specific regions as spam by default. Enable **Emails with this character set** and click **Antispam: Denied Character Sets**. Each row contains the code for one character set. The allocation of countries to character sets is shown on the **Details** tab. If you have communication partners in any of the countries whose character sets are listed here, change the list as follows:

1. Copy the **Antispam: Denied Character Sets** list under **Dictionaries**.
2. Rename your list.
3. Remove the character sets with the countries of your communication partners from the list.
4. Save the list.
5. Delete the **Antispam: Denied Character Sets** list in the **Advanced Spam Filtering** job and enter your own list under **Definite 'Spam' Criteria - E-mails with this**

character set.

Note: *This function checks only the "charset" e-mail header. Make sure that you have selected only character set list(s) for this option, and not any other dictionary.*

Selecting Servers / Job Details

To select servers and specify job details proceed as described under Selecting Servers and Entering Job Details .

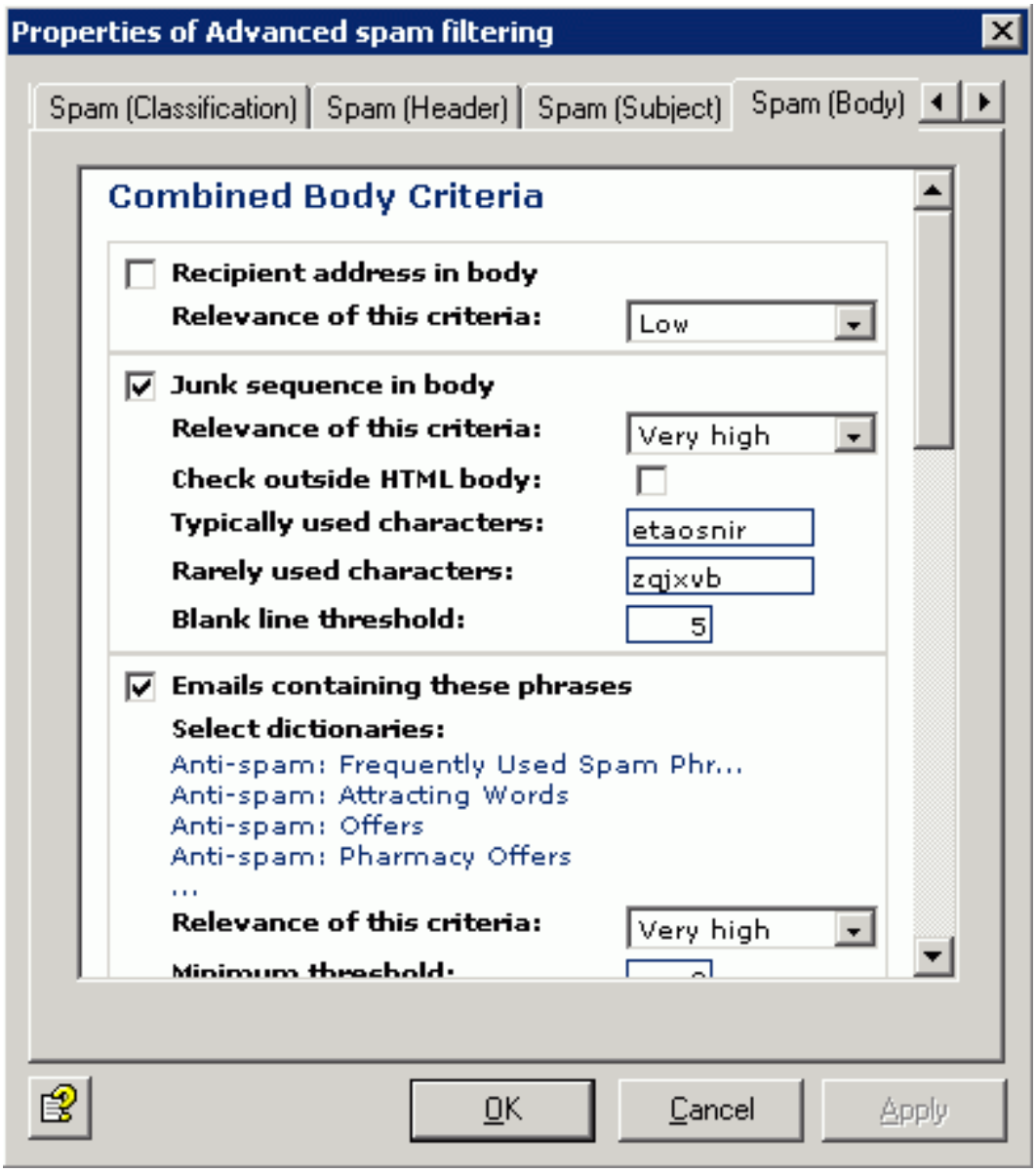
Save the configuration of the AntiVir Exchange Management Console each time you have modified the settings. Click on the **Save** button . The configuration is saved in the `ConfigData.xml` file located in the `Avira\AntiVir Exchange\Config\` folder. Pending changes are indicated by an asterisk (*) next to the top node.

5.4.5 Advanced Spam Filtering

Use the Spam Filtering job to set definite and combined spam criteria. The **definite criteria** classify e-mails as spam or non-spam and label them “Spam Probability is 0% = **None**” or “Spam Probability is 100% = **High**”. The **combined criteria** are used only for e-mails that were not already classified with the definite criteria. For spam detection with combined criteria, several analysis mechanisms (criteria checks) are performed simultaneously and later cross-evaluated. Each criterion has a defined relevance to the overall result, which can be set from **Low** to **Very high**. You can also disable the criterion by deselecting the checkbox. An additional individual value can be assigned to most criteria for **Minimum** and **Maximum**. These two values apply, for example, to the dictionaries used by the criterion to check the e-mails. Below the minimum value, this criterion is not used in the overall weighting of e-mail. When the maximum score is reached or exceeded, **this criterion** considers the e-mail as spam.

Attention: This classification as spam only applies to this one criterion*, whose maximum value was reached while analyzing an mail. As this analysis uses combined criteria, however, the other criteria can yield different results, overruling the criterion whose maximum value was reached. Also refer to the example below.*

Combined Criteria – Example



In the combined criterion **Emails containing these phrases** under the **Spam (Body)** tab, you are using the **Anti-spam: Frequently Used Spam Phrases** dictionary to check the e-mail bodies of all inbound e-mails for spam. This dictionary has a weighting value of 5. If a word or phrase from this dictionary is found in an e-mail, for instance “check it out”, it receives a score of 5. Now specify the number of occurrences required for this criterion to be taken into account in the overall score (**Minimum threshold**) as well as the maximum number of occurrences allowed (**Maximum score**). To do so, add up the value of the words to be found. If, for instance, you specify a value of 30 (as in our pre-configured job), six different words from this dictionary must be found in the message for the message to be classified as spam according to this criterion. If only three words are found, the message is not definitely spam according to this criterion, but the probability of it being spam is already quite high. If the dictionary had a threshold value of 10, three hits would be enough to classify the e-mail as spam.

Note: *Words that occur more than once in an e-mail are counted only once. If, for example, the phrase “check it out” occurs three times within the same e-mail, it would add only 5 to the score, not 15 (as in a normal Wall Content Filtering job).*

In addition, specify the **Relevance of this criteria**, which determines the extent to which the criterion is taken into consideration in the overall evaluation. If set to **Very high**, the

criterion will be taken into account accordingly for the overall value.

Combination of Values to Overall Spam Probability

The individual values of all combined criteria are weighted according to their defined relevance to establish a final evaluation. The job compares this overall value (the spam probability of the message) with the three threshold values and allocates the e-mail accordingly to one of the four spam probability ranges (**None** to **High**). When all combined criteria are taken into account, our sample e-mail with the three words from the dictionary may, therefore, still be classified as spam.

In this example, the e-mail in which six words from the dictionary were found, and which was consequently classified as spam according to this criterion, can still fall into spam probability category **None** or **Low** when the other criteria are considered.

The overall value is calculated from the relevance of the criteria, the minimum and maximum values and the individually set spam probability ranges.

You will find the individual combined criteria on four tabs under **Advanced Configuration**.

The following tables provide an overview of the combined criteria contained in the job.

Note: *For further information on combined criteria, refer to the technical whitepaper or contact our Support.*

Combined No Spam Criterion

Criterion	Description
Emails containing these phrases	Checks whether message bodies contain business words that are typical for the user.

Combined Classification Criteria

Here the results of other spam filtering products – which often use only a single junk filtering method – are included. Their combination with other criteria in the Wall Spam Filtering job eliminates the disadvantages of these products.

Criterion	Description
Exchange SCL value	Also refer to Definite No-Spam Criteria and Write spam result in Exchange SCL field The Intelligent Message Filter (IMF) also determines a spam probability for each message. the so-called Spam Confidence Level (SCL) – from -1 to 9. The higher the spam probability, the larger the SCL. This criterion can be used to include the SCL value in the Avira AntiVir Exchange spam evaluation. For further information refer to http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/imfdeploy.mspx

Criterion	Description
Avira SPACE results	Avira SPACE checks incoming mail against known spam patterns.

Combined Header Criteria

Criterion	Description
Suspicious sender properties	Checks whether the message has a “From” header and whether this header is completed and corresponds with the sender in the SMTP protocol.
Suspicious recipient properties	Checks whether the message contains a “To” header, whether this header is completed and whether it or the “CC” header contains at least one of the SMTP recipients.
Digits in sender address(es)	Checks whether one of the sender addresses (SMTP or mail header) contains digits.
Number of recipients per e-mail	Checks the number of recipients of an e-mail.
Known spam x-mailer	Checks whether the X-Mailer entry in the message is a known spam mail client.
Known spam results	Takes into account the result of a preceding spam analysis for the classification of e-mails as spam or non spam. The result (number of **spam characters** found) is written to the X-header of the e-mail. Avira AntiVir Exchange analyzes the **X-header** and writes the number of **spam characters** into the criterion. The evaluation is performed on the basis of the **minimum/maximum number** of spam characters. The result may come from an external system or be determined by an Avira AntiVir Exchange system on another server.

Combined Subject Criteria

Criterion	Description
Missing subject	Checks whether the message has a subject field with content.
Recipient address in subject	Checks whether the part before the @ of a recipient address is found in the subject of the e-mail.
Junk sequence in subject	Checks whether the e-mail subject contains long strings of spaces or meaningless character strings.
Emails containing these phrases	Checks whether the e-mail subject contains words typically found in spam mail.
Emails containing these concealed words	Checks whether the e-mail subject contains any concealed words from the dictionaries specified.

Combined Message Body Criteria

Criterion	Description
Recipient address in body	Checks whether the part before the @ of a recipient address is found in the message body of the e-mail.
Junk sequence in subject	Checks whether the e-mail body contains long strings of spaces or meaningless character strings.
Emails containing these phrases	Checks whether the e-mail body contains words typically found in spam mail.
Emails containing these concealed words	Checks whether the e-mail body contains any concealed words from the dictionaries specified.
Emails containing suspicious HTML code	Checks whether the e-mail body contains any HTML constructs.
Emails containing suspicious HTML links	Checks whether the e-mail body contains any spammer links.
Many HTML Links	Checks whether the e-mail body contains many HTML links in relation to the size of the text.
Embedded images	Can be used to identify spam content conveyed through embedded images (internal ref. to attachments). For instance, it is possible that (in configurations without SPACE) e-mails with embedded images are systematically considered spam, unless embedded images are standard practice for e-mail communication in the corresponding environment.

5.4.6 Manual Spam Filtering Configuration

To use the **Wall Spam Filtering** job as described above, you should set up the following sequence of actions in your job to ensure effective spam blocking:

1. Filtering of known spam addresses.
2. Checking Subject line for text and obvious elements, such as dots or spaces. Also refer to the **Spam Content (Subject)** dictionary under **Dictionaries** in the **Basic Configuration**.
3. Checking e-mail body texts for spam links (including redirections and click trackers). Also refer to the **Spam Content (Body)** dictionary under **Dictionaries** in the **Basic Configuration**.
4. Checking e-mail bodies for spam text and typical features, such as HTML comments within an HTML message text. Also refer to the **HTML Spam Detector** dictionary under **Dictionaries** in the **Basic Configuration**.

To optimize filtering, be sure to set the most efficient Job Processing Sequence .

5.5 Using SPACE for Fighting Spam

SPACE (= Spam and Phishing Advanced Crossplatform Engine) is an interface used for fighting against Spam and Phishing e-mails. It is used as additional spam criterion in the advanced AntiVir Wall Spam Filtering job.

The **SPACE Engine** analyses the emails using the local information stored in its databases (updated periodically) and several RBL DNS Servers (Realtime Black List).

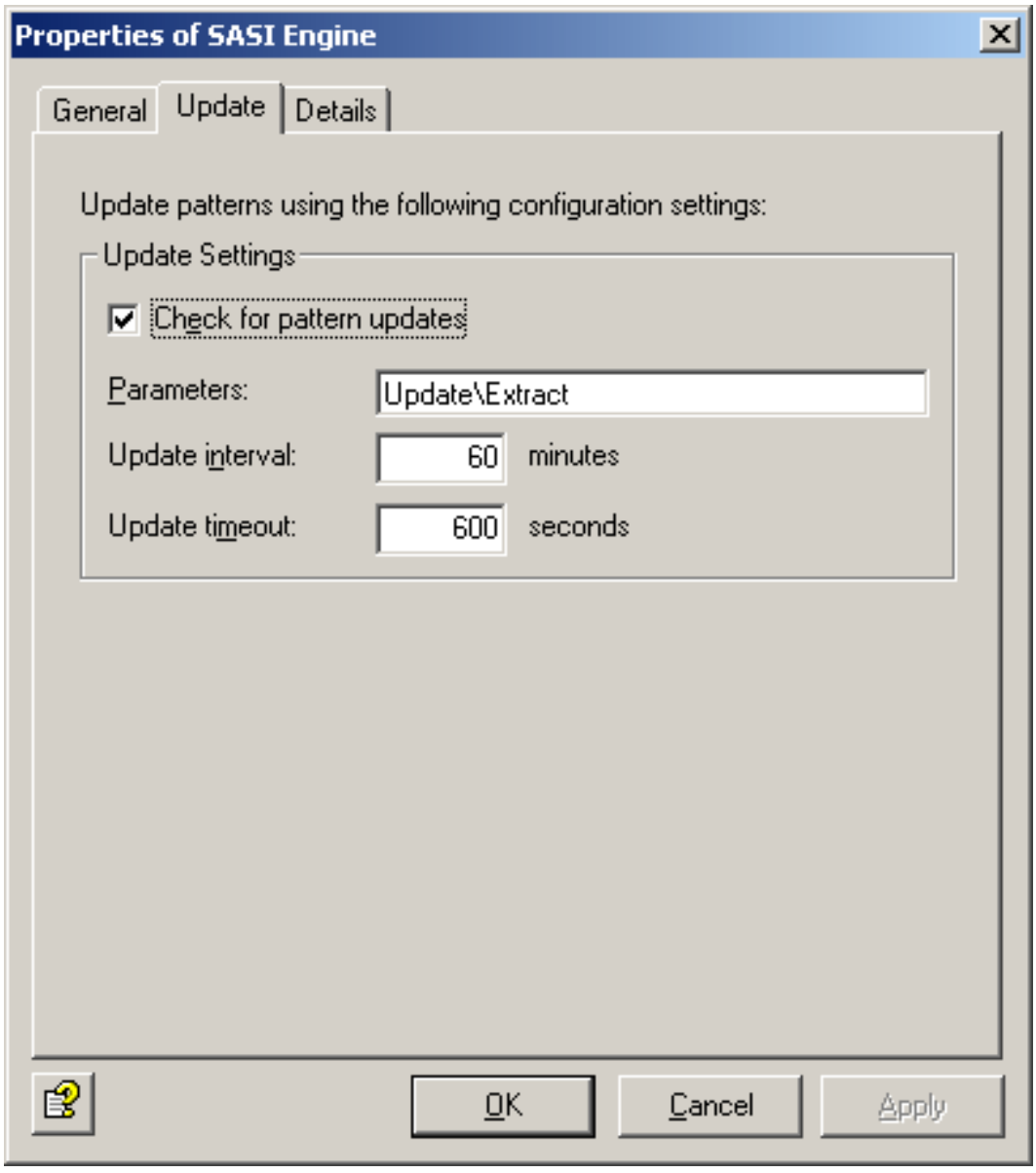
The result of this analysis is a value that is used to calculate the spam probability within the advanced spam filtering job.

5.5.1 SPACE Engine Configuration

If you plan to use SPACE for fighting spam, first configure the SPACE Engine for periodical updates. The configured engine is automatically used whenever a spam filtering jon with SPACE enabled is called.

Open the **Basic Configuration --> Utility Settings** and select **SPACE Engine**. Double-click the selected **SPACE Engine** or right-click and open the **Properties**.

Update Settings (SPACE Update)



Under normal circumstances all you need to set on this tab is the update interval:

- **Parameters**

This field specifies the directory where the update patterns are stored. only change this setting if you have selected another directory during the SPACE setup.

- **Update interval**

  Interval in minutes at which the program checks for pattern updates. The minimum value is 15 minutes.

- **Update timeout**

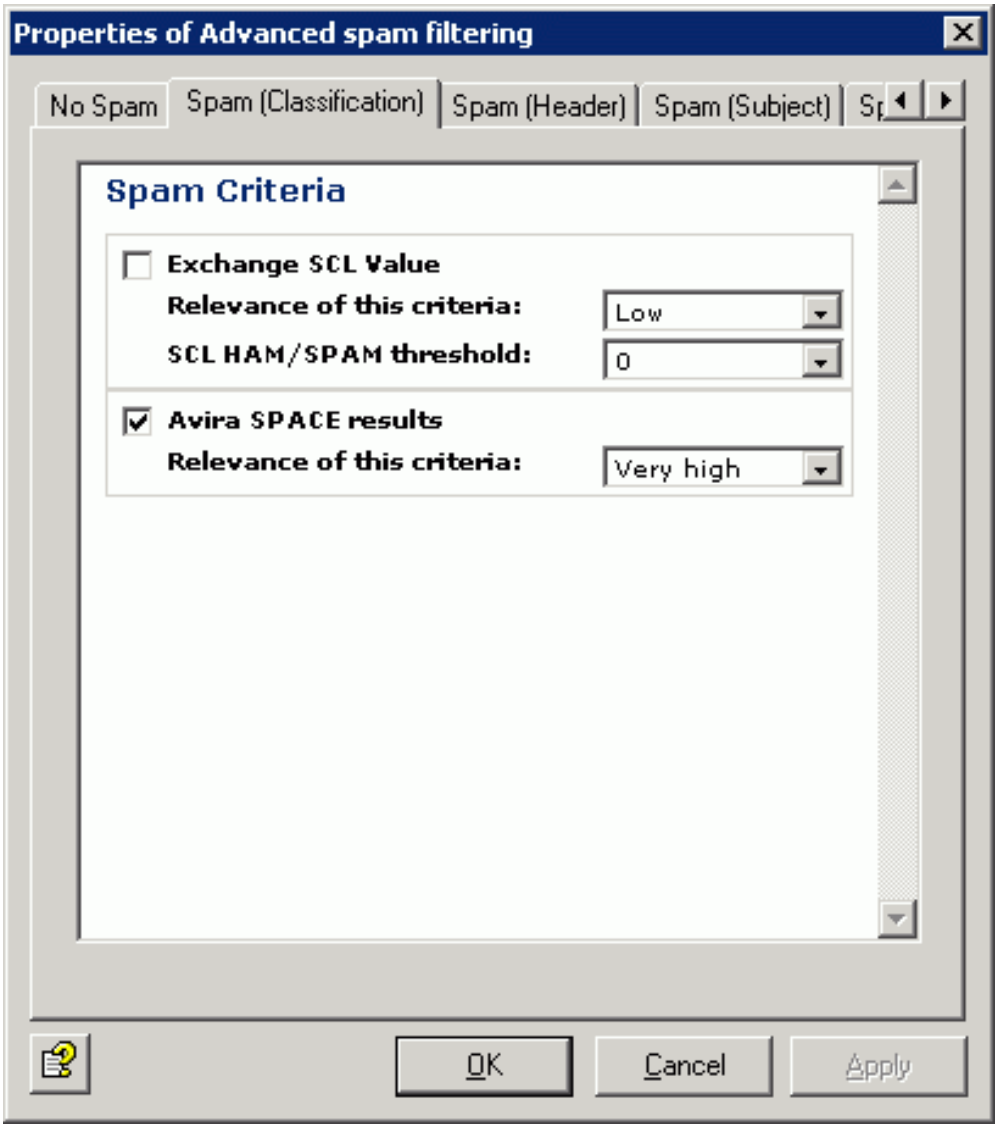
  Timeout (in seconds) for accessing the server. If unsuccessful, the update is aborted after this time has elapsed.

Details

For details on entering the job details refer to Entering Job Details .

5.5.2 Advanced Spam Filtering Job Configuration

1. Under **Mail Transport Jobs** open the **Advanced spam filtering** job. Enable the job and keep the default settings.
2. Under the **Actions** tab, select **Combined Criteria --> Spam (Classification)** and enable the criterion **Avira SPACE results**. Again, it is recommended not to change this setting.



- **Relevance of this criteria**: Set the relevance (weighting) for the entire criterion (ranging from Low - Very high). The values for the relevance and the coefficient are multiplied and yield the result for this criterion.

3. Once this job is active, the configured SPACE Engine is automatically enabled.

5.6 Blocking Images

This job type is used to block images with offensive or pornographic content. Supported formats include:

- JPEG
- GIF
- TIF
- PNG
- BMP

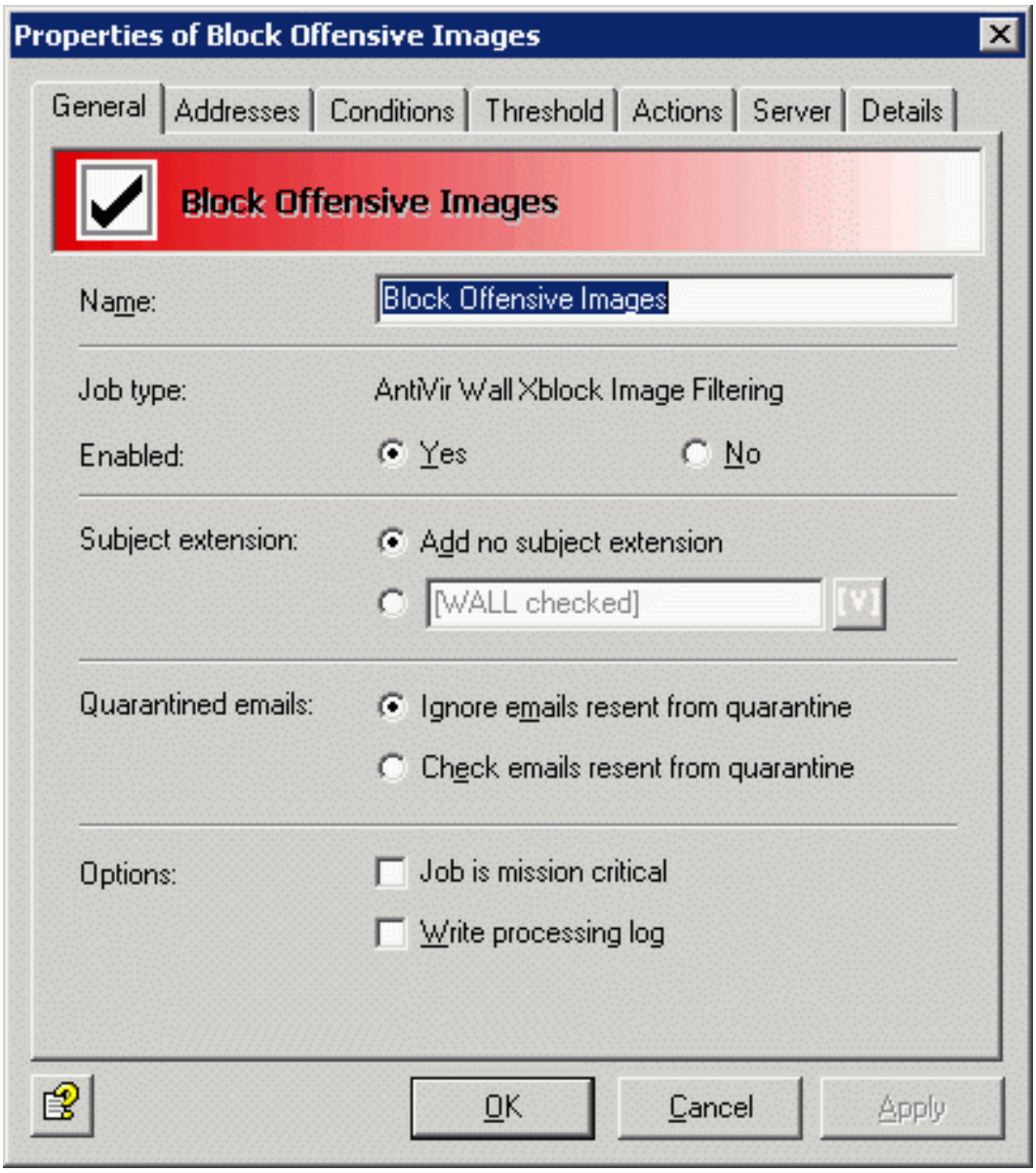
Blocking Offensive Images - Example

Under **Policy Configuration - Job Templates**, you will find the **Block Offensive Images** job. Drag this job to the **Mail Transport Jobs** folder and open it there with a

double-click.

General Settings

Under the **General** tab, enter a name for the job. An active (enabled) job has a checkmark in the job symbol. Set the job to **Enabled: Yes**. Once you have saved your settings with **Apply** and closed the job, the job is enabled.



By default, the **Subject extension** is pre-set to **WALL checked**. If enabled, this text is added to the subject of each e-mail checked by the job.

This job does not process mails that are being resent from **Quarantine (AntiVir Monitor - <select quarantined e-mail> - All Tasks - Resend quarantine item)**, even if the **Resubmit the email to all AntiVir jobs** has been enabled. The **Ignore emails resent from quarantine** option means that this job is systematically skipped when a mail is resent from Quarantine.

For further information on sending quarantined mail, refer to Sending From Quarantine .

For details on the **Mission Critical** option, refer to This job is mission-critical in the "AntiVir" Chapter.

Setting up Address Conditions

Under the **Addresses** tab, specify the senders or recipients to which this job is to apply. You can select addresses from existing lists or from your own ones. For details on how to make the best use of address lists and details, refer to the description under Address Lists .

Setting up Content Conditions

Under the **Conditions** tab you can set the requirements as to which mails or documents a job is to be run for.

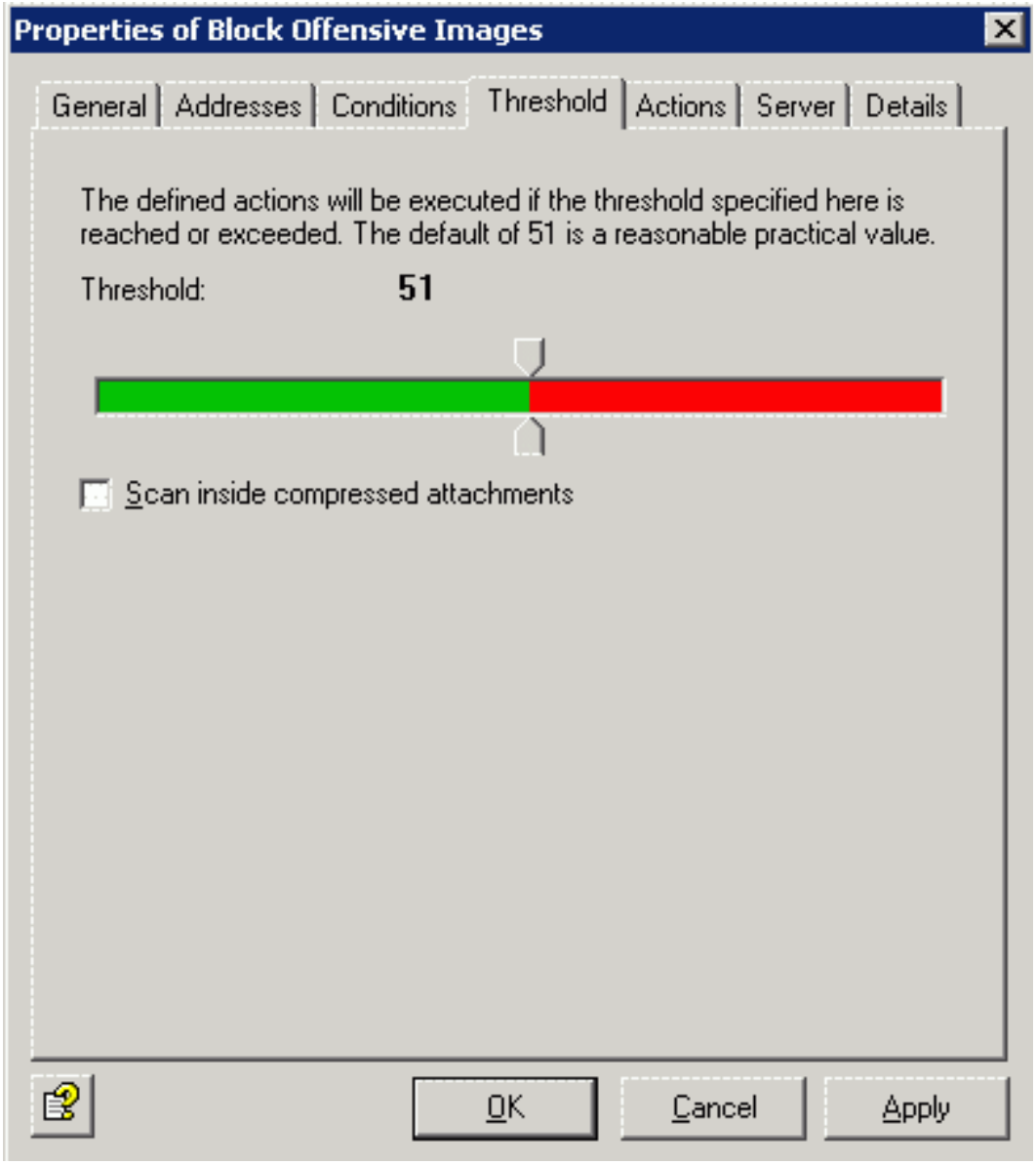
For the use and settings of conditions refer to Conditions .

Note: *The content conditions and the address conditions set in the* ***Addresses*** *tab must simultaneously come true, for a job to be run (logical AND).*

Setting Threshold

Under the **Threshold** tab, set the threshold for triggering the actions defined. To do so, drag the slider with the mouse to the desired position.

Tip: *Alternatively you can use the cursor keys (left/right) to increase/decrease the value in steps of 2. With the Shift key kept depressed at the same time, the value is increased/decreased in steps of 5.*



Whether or not an image is classified as offensive depends on the threshold set here. Possible values range from 0 to 100. Theoretically, "genuine" pornographic or hardcore images can reach a value of 100. In practice however, these values lie between 35 and 65.

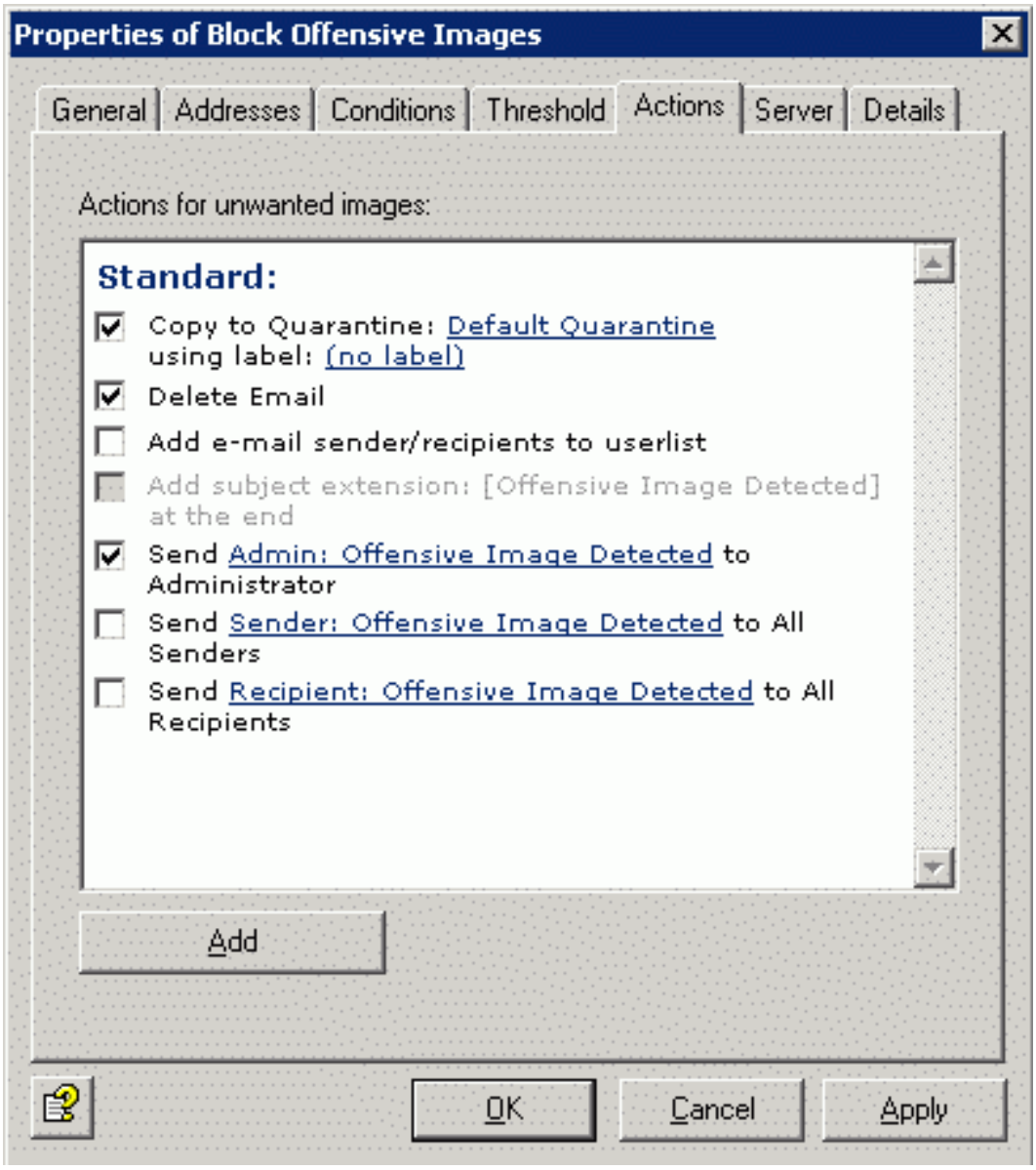
More than 80 % of all images reach values between 45 and 50. We therefore recommend to set the threshold to 51. This value will identify images with "a lot of naked skin" such as pin-ups. A threshold below 50 does not make sense, as these images are likely not to be pornographic. In this example, the action defined is triggered when the threshold of 51 is reached or exceeded. The overall result for the e-mail is the highest value of all images attached.

E-mails with images that could not be classified (e.g. charts) are delivered to the recipient, unless they also contains images that could be classified and have reached the threshold.

Scan inside compressed attachments means that the internal unpacker extracts files from archives and checks them for unwanted images. If this option is disabled, only the archive is checked and identified as compressed format.

Defining Actions

Under the **Actions** tab, define the actions to be performed when the job finds an e-mail with one or more offensive images.



In this example, a copy of the message is placed in Quarantine and the message is deleted **without** being delivered to its recipient. A notification warning of the denied address is sent to the Administrator. You can select this notification from the pull-down menu of available notification templates, which you can format using the HTML toolbar or by entering appropriate HTML code yourself.

Note: *If the job identifies more than one offensive image, the notification variables* ***Xblock attachment and Xblock result*** *will provide the name and the analysis result for the image with the highest score only.*

To define further actions, click the **Add** button.

For a description of the procedure, refer to the description in the AntiVir chapter under Enabling Virus Scanning - Example, "Defining Actions" .

5.7 Limiting the Number of Recipients

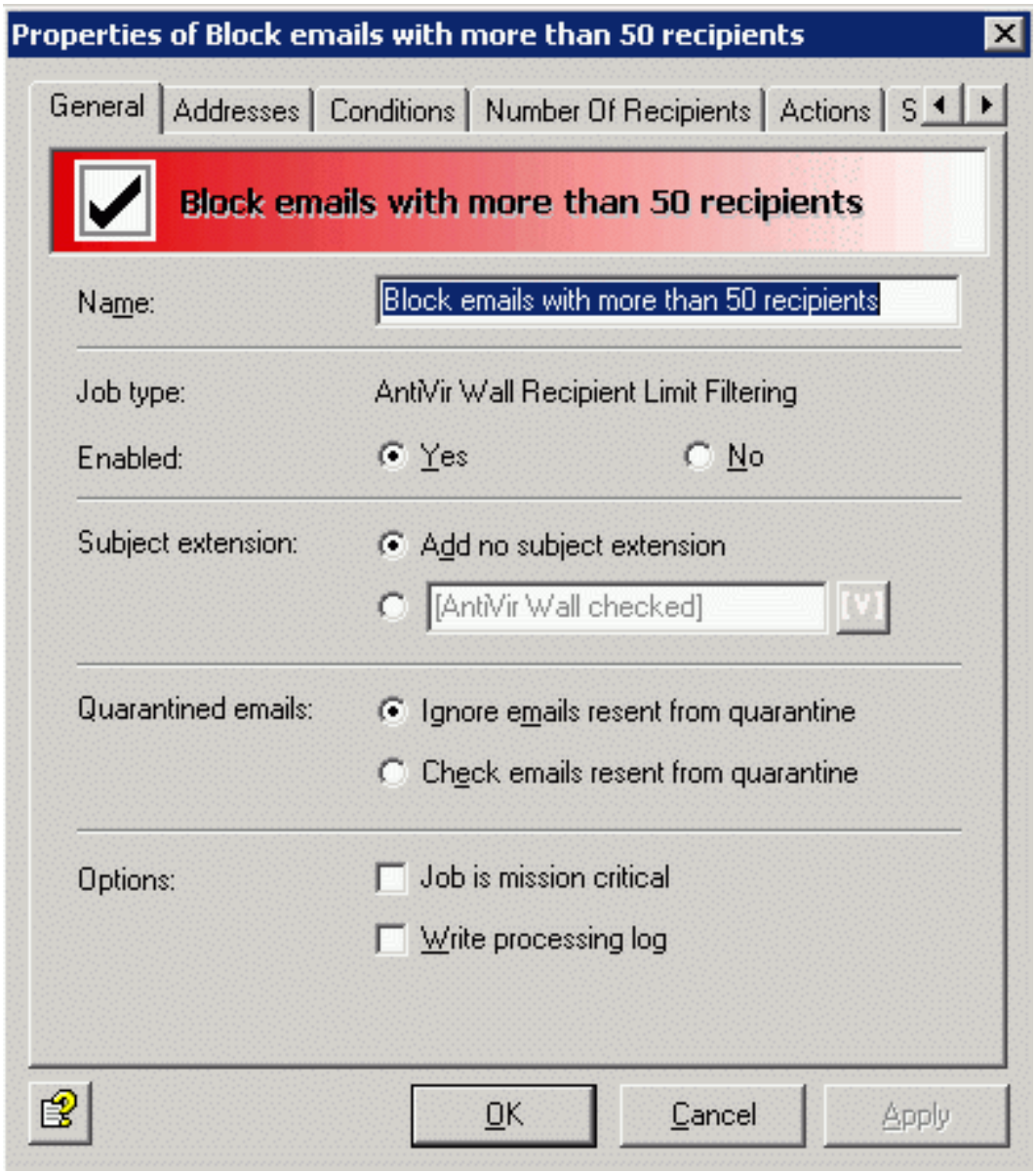
With this job type, you can limit the number of recipients for each e-mail. When this job is enabled, users cannot send bulk mail to all users in your company.

Limiting Number of Recipients - Example

Under **Policy Configuration - Job Templates** you will find the **Block emails with more than 50 recipients** job. Drag this job to the **Mail Transport Jobs** folder and open it there with a double-click.

General Settings

Under the **General** tab, enter a name for the job. An active (enabled) job has a checkmark in the job symbol. Set the job to **Enabled:Yes**. Once you have saved your settings with **Apply** and closed the job, the job is enabled.



By default, the **Subject extension** is pre-set to **AntiVir Wall checked**. If enabled, this text is added to the subject of each mail checked by the job.

This job does not process mails that are being resent from **Quarantine (AntiVir Monitor - <select quarantined e-mail> - All Tasks - Resend quarantine item)**, even if the **Resubmit the email to all AntiVir jobs** has been enabled. The **Ignore emails resent from quarantine** option means that this job is systematically skipped when a mail is resent from Quarantine.

For further information on sending quarantined mail refer to Sending From Quarantine .

Setting up Address Conditions

Under the **Addresses** tab, specify the senders or recipients to which this job is to apply. You can select addresses from existing lists or from your own ones.

For details on how to make the best use of address lists and details, refer to the description under Address Lists .

Setting up Content Conditions

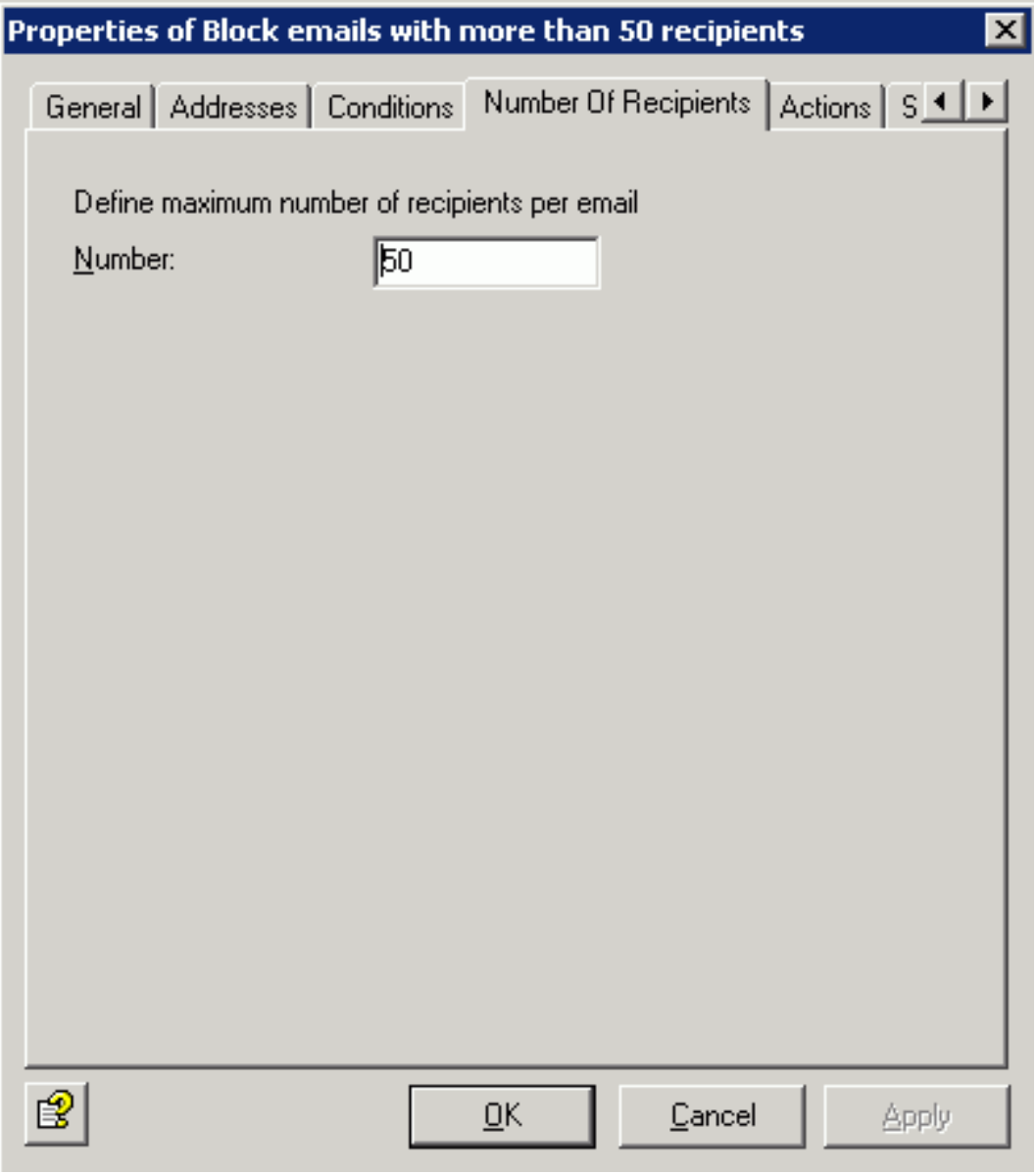
Under the **Conditions** tab you can set the requirements as to which mails or documents a job is to be run for.

For the use and settings of conditions refer to Conditions .

Note: *The content conditions and the address conditions set in the* ***Addresses*** *tab must simultaneously come true, for a job to be run (logical AND).*

Specifying the Number of Recipients

Under the **Number Of Recipients** tab, enter the maximum number of recipients per e-mail:

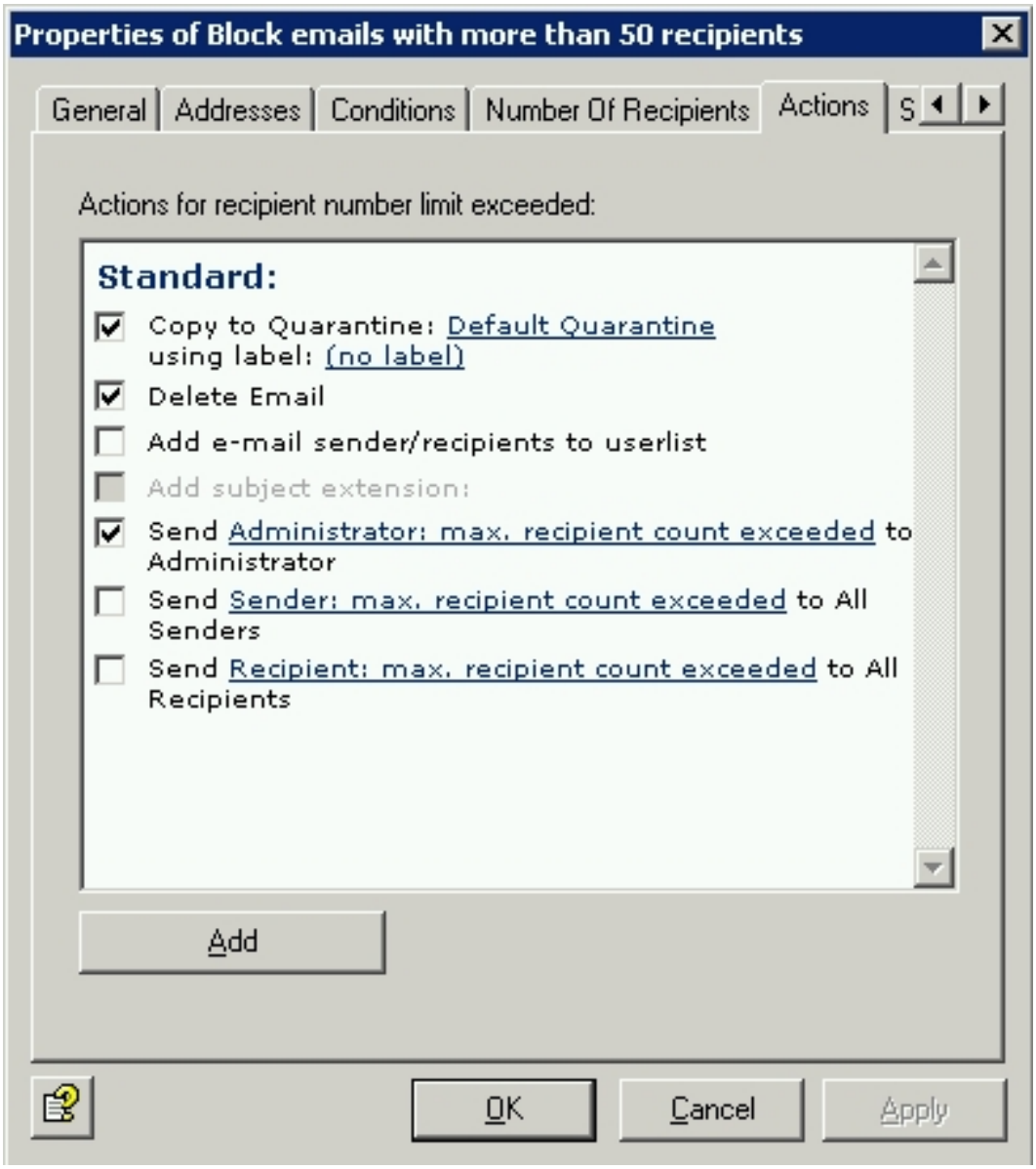


In this example, each incoming or outgoing e-mail can be addressed to no more than 50 recipients. As soon as an e-mail contains 51 recipients, the specified action is triggered.

Note: *If an e-mail is addressed to a group of recipients with a single address, the Exchange server must be able to resolve the list into its individual recipients to identify the actual number of recipients. Addresses that act as mailing lists are treated as single addresses if they are outside the scope of the Exchange server.*

Defining Actions

Under the **Actions** tab, specify the actions to be taken **when the job finds a mail with too many recipients**.



In this example, a copy of the message is placed in Quarantine and the message is deleted **without** being delivered to its recipients. A notification about the number of recipients is sent to the Administrator. You can select this notification from the pull-down menu of available notification templates, which you can format using the HTML toolbar or by entering appropriate HTML code yourself.

To define further actions, click the **Add** button. For a description of the procedure, refer to the description in the AntiVir chapter under Enabling Virus Scanning – Example, "Defining Actions" .

Selecting Servers/ Job Details

To select servers and specify job details proceed as described under Selecting Servers and Entering Job Details .

Avira AntiVir Exchange 7

Avira AntiVir Exchange 2000/2003
Avira AntiVir Exchange 2007

Avira GmbH

Lindauer Str. 21
88069 Tettnang
Germany
Telephone: +49 (0) 7542-500 0
Fax: +49 (0) 7542-525 10
Internet: http://www.avira.com

© Avira GmbH. All rights reserved.

This manual was created with great care. However, errors in design and contents cannot be excluded. The reproduction of this publication or parts thereof in any form is prohibited without previous written consent from Avira GmbH.

Errors and technical subject to change.

Issued Q3-2009

AntiVir® is a registered trademark of the Avira GmbH.
All other brand and product names are trademarks or registered trademarks of their respective owners. Protected trademarks are not marked as such in this manual. However, this does not mean that they may be used freely.